Képzés megnevezése	**Tudatos szociális médiafogyasztás**

A tananyagegységek

	A tananyagegység megnevezése
1.	Hogyan hat ránk a média, hatás-befogadás elméletek
2.	Biztonságos internethasználat
3.	Valós vs digitális/ál- identitás
4.	Forráshasználat és kritika: hírek és álhírek megkülönböztetése
5.	Darknet, becserkészés, cyberbullying, online predátorok, gyűlöletbeszéd
6.	A Facebook tudatos használata
7.	Az Instagram tudatos használata
8.	Youtube tudatos használata
9.	LinkedIn tudatos használata

1. tananyagegység

Megnevezése	Hogyan hat ránk a média, hatás-befogadás elméletek

A médiahatások kérdése

A média és a közönség viszonyának egyik legfontosabb kérdése az, hogy a média befolyásolja-e – és ha igen, miként – az emberek gondolkodását és viselkedését. Pontosabban: az nyilvánvaló, hogy a modern tömegkommunikációs eszközök megjelenése megváltoztatta valamennyiünk életét. A média vált a legfontosabb információforrásunkká. Azt is tudjuk, hogy nagymértékben átalakította szabadidőnk eltöltésének módját. A média hatásai közül az alábbiakban csak egyről: a médiának az emberek véleményére és viselkedésére gyakorolt hatásáról lesz szó.

Az, hogy a döntéseinkhez (tehát a véleményünk és a magatartásunk meghatározásához) szükséges információkat a médiából merítjük, önmagában csak azt jelenti: a világról való tájékozódásunk korábbi forrásainak, például az iskolának és a templomnak a szerepét mind jobban átvette a média – hiszen korábban is csak tudásunk töredékére tettünk szert személyes tapasztalás útján.

Az, hogy a média vált a legfontosabb információforrásunkká, önmagában még aligha indokolja a médiahatás kérdésének felvetését, hiszen többé-kevésbé világosan megkülönböztethetjük a tájékoztatást a befolyásolástól. A *tájékoztatás* esetében az üzenet címzettje józan megfontolások alapján mérlegel és dönt arról, hogy megváltoztatja-e a véleményét és a magatartását, vagy sem. A *befolyásolás* esetében viszont az üzenet címzettjének a kommunikátor akaratának megfelelően változik a véleménye és a viselkedése. A kérdés tehát az, hogy a média képes-e *a kommunikátor akaratának megfelelő* vélemény- és viselkedésváltozást kiváltani, vagyis – határozottabban fogalmazva – képes-e manipulálni az embereket, azaz képes-e őket anélkül befolyásolni, hogy a befolyásolási szándék tudatában lennének. Másképpen: ki vagyunk-e szolgáltatva a média „hatalmának”? A közkeletű nézet szerint a média nagy hatást gyakorol a társadalomra. E nézet általános elfogadottságát jelzi egyebek mellett a médiával egyidős cenzúra és propaganda: a média nagy hatását feltételezve a cenzúrával egyes nézetek terjedésének igyekeztek gátat vetni, a propagandával bizonyos nézeteket kívántak terjeszteni. A *médiapesszimisták* szerint a média zömmel káros hatást gyakorol a társadalomra; például az offenzív politikai propaganda és a gyűlöletbeszéd felel az emberek közötti gyűlölködésért, a pornográfia a családi kapcsolatok fellazulásáért, a médiaerőszak a való világban tapasztalható vagy tapasztalni vélt erőszak elharapózásáért. A *médiaoptimisták* ellenben azt várták a médiától, hogy majd elviszi a tudást, az ízlést és a morált az otthonokba, nemesítve a társadalmat. A média hatásának kérdése mindamellett különösen a politikai propaganda és kampány, a médiaerőszak és a gyűlöletbeszéd kontextusában merül fel, azaz az emberek többsége úgy véli: a média nagy és döntő módon káros hatást gyakorol a társadalomra.

Vajon igazuk van-e azoknak, akik nagy és káros társadalmi hatást tulajdonítanak a médiának? A kérdés megválaszolása azért is fontos, mert akkor, ha e nagy és káros hatás bizonyítható, indokolt lehet a média szigorú szabályozása, hiszen az államnak kötelessége megvédeni polgárait a rájuk leselkedő veszélyektől. Ha azonban az bizonyul be, hogy a média társadalomra gyakorolt hatása csekély, akkor nehezen indokolható a szólás szabadságának csorbítása.

Hatás- és befogadásvizsgálatok

Az alábbiakban kronologikus rendben haladva azokat a tudományos igényű elméleteket és empirikus vizsgálatokat vesszük át, amelyek e kérdést igyekeztek megválaszolni, és amelyeket a médiahatás-kutatás és a befogadásvizsgálatok mérföldköveinek tekintenek (vagyis amelyekre a leggyakrabban hivatkoznak a különböző szakirodalmi források). Végül összegzem a különböző elméletek közös vonásait és a kutatások ma rendelkezésre álló következtetéseit.

1. A lövedékelmélet

Az 1920-as és az 1930-as évek közgondolkodását és tudományos gondolkodását a lövedékelmélet *(bullet theory)*jellemezte. Eszerint a média nagy és közvetlen hatást gyakorol az emberekre: a médiából – ekkoriban a nyomtatott sajtóból, a filmből és a filmhíradóból, a köztéri plakátokból, valamint a rádióból – érkező üzenetek lövedékként csapódnak a közönség testébe, maradandó elváltozást okozva benne. A lövedékelméletet nevezik

injekcióstű-elméletnek *(hypodermic model)* is, arra utalva, hogy a média az üzeneteket injekciós tűként fecskendezi az emberek bőre alá, azaz a média nagy és közvetlen (direkt) hatást gyakorolna a közvéleményre.
A lövedékelmélet a tömegkommunikációt olyan egyirányú folyamatként (médiainger – közönségválasz) írja le, amelyben a közönség passzív és kritikátlan szerepet játszik, és nincs módja az aktív visszacsatolásra, a média befolyásolására. A közönséget olyan egynemű masszának tételezte, amelynek valamennyi tagja egyformán reagál a lövedékként rá záporozó üzenetekre. A korabeli társadalomelmélet ténynek tekintette a személyes kötelékek meglazulását, a hagyományos identitások felbomlását, a társadalom atomizálását (a „magányos tömeg" megjelenését), ezért úgy vélte: a közönség különösen kiszolgáltatottá válik a média manipulációs törekvéseinek. Ezt az elméletet megerősíteni látszott az is, hogy az 1930-as években Európa totális államaiban – különösen a hitleri Harmadik Birodalomban és a sztálini Szovjetunióban – a politikai hatalom korábban ismeretlen mértékben élt a propagandával, támaszkodva a modern tömegkommunikációs eszközökre, elsősorban a rádióra, hamarosan újabb háborúba sodorva a világot. A média nagy hatásának közkeletű példája az 1938-ban bemutatott rádiójáték, a *Világok harca* is. Az amerikai Orson Welles fikciós műve a hírműsorok eszközeivel ábrázolta a „marslakók" Egyesült Államok elleni támadását. A korabeli sajtóbeszámolók szerint a rádiójáték hatására pánik tört ki azok körében, akik a műsor bevezetőjét nem hallották, és azt hitték: valós eseményekről szóló beszámolót hallgatnak.

2. A kétlépcsős hatás modellje
Az 1940-es években új elmélet jelent meg a tudományos igényű vizsgálatokban: a kétlépcsős hatás *(two-step flow of influence)* modellje, amely szerint a média csak kismértékben és közvetett módon képes befolyásolni a közvéleményt.
Paul Lazarsfeld és munkatársai úgy vélték: a közönség nem homogén masszaként reagál a médiából felé záporozó üzenetekre, hanem mindenki a maga módján fogadja be őket, hiszen a média hatását más hatások keresztezik (azaz a médiainger – közönségválasz-modellt újabb változókkal kell kiegészíteni). Lazarsfeldék úgy vélték: a média csak áttételesen, két lépcsőben befolyásolja a választók gondolkodását. Az emberek elsősorban a környezetükben élő véleményvezérekre – például a család vagy a munkahely valamely tekintélyes tagjára – hallgatnak, azaz a személyközi kommunikáció véleménybefolyásoló hatása nagyobb, mint a tömegkommunikációé. A véleményvezérek ugyanakkor elsősorban a médiára támaszkodva alakítják ki a maguk véleményét, így – korlátozott mértékben és áttételesen – a média mégiscsak hatást gyakorol az emberekre.

3. A szelektív észlelés elmélete
A szelektív észlelés *(selective perception)* elmélete arra a kérdésre keresett választ, hogy miért korlátozott a média társadalomra gyakorolt hatása, azaz miért alacsony hatásfokúak a politikai kampányok.
Az emberek szelektálnak a rájuk záporozó üzenetek között. Keresik azokat az üzeneteket, amelyek megerősítik létező véleményüket, és kerülik azokat, amelyek ellentmondanak neki. A szelekció három szintjét különböztethetjük meg:

- a szelektív válogatás azt jelenti, hogy az emberek eleve nem követik figyelemmel azokat az újságokat és műsorokat, amelyekről tudják, hogy a saját véleményükkel szembenálló véleményeket fogalmaznak meg vagy ilyen véleményekre támaszkodnak;
- a szelektív észlelés azt jelenti, hogy – ha bele is szaladnak a saját véleményüknek ellentmondó üzenetekbe – azokat elengedik a fülük mellett; végül
- a szelektív emlékezés azt jelenti, hogy ha véletlenül bele is szaladnak a saját véleményüknek ellentmondó üzenetekbe, és azokat meg is jegyzik, akkor is hamarosan elfelejtik őket.

Ennek az a magyarázata, hogy az ember kerüli a disszonáns helyzeteket, azaz igyekszik megszabadulni mindazoktól az információktól és véleményektől, amelyek saját, gondosan felépített világképének újragondolására késztetnék, mert világképének újragondolása túlságosan sok kognitív energiáját kötné le.

4. A kultivációs elmélet
Az 1970-es évek meghatározó médiahatás-elmélete George Gerbner magyar származású amerikai médiakutató kultivációs teóriája *(cultivation theory)* volt, amely ismét a média nagy társadalmi hatását látta igazoltnak. Az új elmélet megjelenésében szerepet játszott az is, hogy ekkorra terjedt el a televízió, amelynek a közvéleményre gyakorolt hatása is nagyobbnak látszott, mint az addig egyeduralkodó nyomtatott sajtóé és a rádióé. Gerbner úgy vélte: a televízió – amely információforrásként fontosabbá vált, mint a személyes tapasztalat – nemcsak tükröt tart a „valóság" elé, de formálja is azt: a valóság képeit bizonyos szabályok mentén rakja újra össze, új (virtuális) valóságot teremtve. A média szelektív: a valóság bizonyos elemeit kultiválja (előnyben részesíti), míg másokat a háttérbe szorít. A média hatására mindazok, aki sok időt töltenek a képernyő előtt, fokozatosan elfogadják a valóság televízióban ábrázolt képét a „valóság" hű reprezentációjaként.
Az erős és a gyenge tévénézők világképét összevetve azt tapasztalta, hogy azoknak, aki sokat tévéznek, jobban hasonlít a világképük a tévében közvetített világképhez – hajlamosak például alulbecsülni a feketék számát, de túlbecsülni a fekete bűnözők valóságos társadalmi arányát.

Gerbner gyorsan népszerűvé váló elméletét azonban később sokan bírálták. Elsősorban azt rótták fel neki, hogy a mai, sokcsatornássá és sokszínűvé vált televíziós piacon – ahol az egyik csatorna állandóan akciófilmeket, a másik híreket, a harmadik szakácsműsort sugároz – nem beszélhetünk egységes televíziós világképről.

5. A napirendelmélet

Szemben Gerbnernek a média nagy hatását tételező modellek közé sorolható kultivációs elméletével, a néhány évvel később megfogalmazott napirendelmélet *(agenda-setting theory)* ismét a korlátozott hatás iskoláját látszott erősíteni. A média – különösen a hírmédia – elsősorban nem azt szabja meg, hogy mit gondoljunk, hanem azt, hogy miről gondolkodjunk. A média napirendje befolyásolja ugyan a közvélemény napirendjét, de a napirenden szereplő témák értelmezésére már nincs nagy hatással.

„…a hírek kiválasztásával és bemutatásával a szerkesztők, az újságírók, a műsorszolgáltatók fontos szerepet játszanak a politikai valóság formálásában. Az olvasók nemcsak a szóban forgó kérdésről értesülnek, hanem arról is, milyen fontosságot tulajdonítsanak neki."

Az események közötti szelektálással tehát a média fontossági sorrendet állít fel: egyes eseményeket fontosnak, másokat kevésbé fontosnak pozicionál. Az emberek többsége azokat a témákat tartja fontosnak, amelyek a hírműsorok élén és a lapok címlapján szerepelnek, és amelyekről a médiumok nagy terjedelemben számolnak be. Ám azt, hogy az egyes eseményeket miként ítélik meg, a média már nem befolyásolja számottevően.

A média tematizációs *(priming)* szerepének felismerése azóta számottevően befolyásolta a valóságot: a modern politikai kommunikáció egyik célja a sikeres tematizáció, vagyis az, hogy a politikai kommunikátorok a pártjuknak kedvező vagy a politikai ellenlábasaiknak kedvezőtlen témákat tűzzék napirendre.

Az újabb napirendkutatások szerint különbséget kell tenni háromféle napirend: a média, a közvélemény és a politika napirendje között (miközben egyik napirendet sem feltétlenül a „való világban" fontos témák dominálják). E három napirend kölcsönösen és előre nehezen megjósolható módon befolyásolja egymást: a média napirendje nemcsak alakítja, de tükrözi is a közvélemény és a politika napirendjét, és viszont. Mindamellett a három napirend között az empirikus kutatások szerint a média látszik a legbefolyásosabbnak.

6. A framingelmélet

Ha a média napirendje képes befolyásolni a közvélemény és a politika napirendjét, felmerül a kérdés, hogy ki befolyásolja a média napirendjét. Az egyik lehetséges válasz e kérdésre az, hogy a médiabirodalmak tulajdonosai, a hírekben gyakran idézett források és más befolyásos hatalmi tényezők rendelkeznek döntő befolyással a médiában közvetített tartalmakra. A média nagy hatását tételező *framing*elmélet szerint a média a politikai és a gazdasági elitek ellenőrzése alatt áll, míg az egyszerű emberek – pénz, hatalom és szaktudás híján – csak befogadóként férnek hozzá a médiához. Szemben a „tömeggel", az elitek hatékonyan képesek befolyásolni a médiaüzeneteket. A média ezért az üzeneteket – különösen a híreket – nem objektíven ábrázolja, hanem torzítja, azaz olyan értelmezési keretben *(frame)* prezentálja, amely az események egyes elemeit hangsúlyozza, másokat azonban homályban hagy. A politikai problémák bemutatása során így a hírek automatikusan felkínálnak bizonyos értelmezéseket, és előnyben részesítik őket más értelmezésekkel szemben, azaz felkínálnak egy „preferált" olvasatot.

A *framing*elméletet megkérdőjelezi a technológia fejlődése is. A sokcsatornás és sokszínű médiapiacon a professzionális kommunikátorok között megjelentek azok az amatőrök is, akik korábban nem juthattak szóhoz – például a közösségi rádiók mikrofonjánál. És bár e médiumok sosem tartoztak a média fősodrához (azaz közönségrészesedésük elenyésző volt), a valóságértelmezésnek a politikai elitektől független alternatíváit kínálták fel az embereknek. Az internet megjelenése óta a legfontosabb hagyományos médiumok – az újság, a rádió és a televízió – elvesztették információs és véleményformáló hegemóniájukat. A világháló nemcsak az információk több forrásból való ellenőrzésére kínál viszonylag olcsón mindenki számára lehetőséget, de véleményének kifejezésére is, azaz – legalábbis elméletileg – kiegyenlítheti a társadalmi helyzet különbségeiből fakadó hátrányokat.

7. Használat és kielégülés-modell

Ismét a korlátozotthatás-elméletek közé sorolható a néhány évvel később megfogalmazott használat és kielégülés-modell *(uses and gratifications model).* Eszerint az emberek médiahasználatának sajátos, egyénenként eltérő mintái vannak. A befogadóknak különböző szükségleteik, elvárásaik vannak, amelyeket a médiahasználat során elégítenek ki. Másképpen fogalmazva: nem a média használja (befolyásolja) az embereket, hanem az emberek használják a médiát; nem a média formálja a közvéleményt, hanem domináns módon a közönség formálja a maga szükségleteire a médiát. Az emberek aktívan válogatnak, azt a csatornát keresve, amely a legjobban felel meg a szükségleteiknek; ha valamely csatorna ezt nem teszi meg, továbbkapcsolnak.

A média legfontosabb használati módját az alábbiak jelentik:

- a tanulás és az információszerzés: az emberek a televízió segítségével tájékozódnak a világról,
- a szociális kontaktus: az emberek különféle módokon viszonyulhatnak a képernyőn megismert figurákhoz, illetve megbeszélhetik a többiekkel a látottakat,
- az elszakadás: az emberek a televíziót nézve egy időre „elmenekülhetnek" a valóság nehézségei elől,

 a szórakozás és az időtöltés.
A használat és kielégülés-modell szerint tehát a média használata interaktív folyamat, amely mindig az egyéni szükségletekhez, szerepekhez, értékekhez, társadalmi szituációkhoz kötődik. A média használata során a felhasználó aktívan válogat. Bár a médiának lehetnek szándékolatlan hatásai is, csak korlátozott mértékben képes befolyásolni közönségét, mert használata az emberek meglévő elképzeléseihez, attitűdjeihez igazodik.
A használat és kielégülés-modell paradigmaváltást jelzett a média és a közvélemény viszonyát vizsgáló kutatásokban. A kutatások ettől kezdve már nem a *média közönségre gyakorolt hatására* fókuszáltak, hanem arra, hogy miként *használja a közönség a médiát,* azaz milyen körülmények befolyásolják a média használatát. Azt igyekeztek feltárni, hogy milyen tényezők befolyásolják az üzenetek értelmezését.

8. A hallgatási spirál
Az utánfutóhatás *(bandwagon-effect)* vagy„tarts a győztessel"-hatás elmélet szerint akkor, ha az emberek a médiából nyert képek alapján úgy érzékelik, hogy valamely politikai erő nyeri a választásokat, hajlamosak az adott politikai erő híveiként feltüntetni magukat, sőt akár a szóban forgó politikai erőre adni a voksukat, ha egyébként egy másikkal rokonszenveznek. Motivációjuk vagy az elszigetelődéstől való félelem, vagy a „győztes csapathoz" való tartozás vágya. Az elméletet először megfogalmazó és már említett Lazarsfeld és munkatársai (1948) ugyanakkor azt hangsúlyozzák, hogy az utánfutóhatás csak a politika iránt kevésbé érdeklődő és kiforratlan politikai preferenciákkal rendelkező választók esetében érvényesül. A média tehát befolyásolhatja az emberek véleményét és a viselkedését, de csak korlátozott körben és bizonyos körülmények között
Az utánfutóhatás elméletét fejlesztette tovább a média nagy társadalmi hatását tételező elméletekhez való visszatérést jelentő hallgatási spirál *(spiral of silence)* elmélete. Eszerint a média azáltal gyakorol hatást az emberek véleményére és viselkedésére, hogy egyfajta véleményklímát teremt: elhiteti velük, hogy a domináns közvélemény másként gondolkodik, mint ők. Az elmélet szerint azok az emberek, akik úgy érzik, a véleményük megértésre talál a közvéleményben, előszeretettel hangoztatják álláspontjukat, ám azok, akik úgy érzik: „különvéleményt" képviselnek, a társadalmi elszigetelődéstől tartva inkább csendben maradnak vagy megváltoztatják nyilvánosan hangoztatott véleményüket. Másképpen: elválik egymástól az emberek magánszférában – családi, baráti körben – és a nyilvános szférában hangoztatott véleménye. A média tehát azáltal gyakorol hatást az emberekre, hogy azt a benyomást kelti bennük: véleményükkel kisebbségbe szorulnának. Az elmélet azon a feltevésen alapul, hogy az emberek számára fontosabbak társas kapcsolataik, fontosabb az, hogy mások elfogadják őket, mint az, hogy hangot adjanak saját véleményüknek, illetve attól tartanak: véleményük felvállalása kedvezőtlenül befolyásolhatja egzisztenciájukat, karrierjüket. A hallgatási spirál elmélete tehát azt mondja, hogy a média befolyásolja az emberek (nyilvános) magatartását (noha közben véleményük változatlan maradhat).

9. A kódolás-dekódolás modell
A kódolás-dekódolás *(encoding/decoding)* elmélete ismét a korlátozott hatás iskolájába sorolható. Ez abból a megfontolásból indul ki, hogy a szöveg mindig többértelmű, azaz korántsem biztos, hogy az üzenet ugyanazt jelenti a kommunikátor, mint a címzett számára. A szövegnek nincs a befogadótól független jelentése.
A kódolás-dekódolás-modell kiindulópontja szerint a jelentés mindig a használat során jön létre. Egy hír értelmezését meghatározzák egyebek mellett a hírgyártás körülményei (így például az adott médium hírforrásainak száma), az eseményről szóló narratívát befolyásoló érdekcsoportok, a befogadó társadalmi és gazdasági státusa, valamint a befogadás körülményei.
A nézők eltérő értelmezési stratégiákat használnak. Ugyanazt a műsort nézik, mégsem ugyanazt a műsort látják.

10. A performatív hatás modellje
A Csigó Péter magyar médiakutató kifejezésével élve performatívnak nevezett hatás modellje abból az új, sokcsatornás televíziós látképből indul ki, amelyet a kereskedelmi ural. A performatív hatás modellje azt állítja, hogy a néző folyamatos „párbeszédet" folytat a televízióval. Egy műsor csak akkor képes hatást gyakorolni nézőire, ha képes mozgósítani, elkötelezni őket, vagyis a befogadók érzelmi kötődést alakítanak ki a műsorral, azonosulnak vele.

Összegzés
A média és a társadalom viszonya a tömegsajtó és a filmhíradó térhódítása óta foglalkoztatja a kutatókat. A kutatások a médiahatások modelljének a médiainger és a közönségválasz egyirányú kapcsolatára egyszerűsített hatásmodelljétől eljutottak a befogadásvizsgálatokig, amelyek a média és a közönség bonyolult kölcsönhatását igyekeznek feltérképezni. A kutatások – némileg leegyszerűsítve – két „iskolába" sorolhatók: a média nagy és közvetlen hatását tételező *direkthatás-modellek* és a média csekély és áttételes hatását tételező *korlátozotthatás-modellek* iskolájába. E két iskolát nevezik hatásparadigmának és használatparadigmának, illetve a hatás *(influence)* és a kölcsönhatás *(interaction)* iskolájának is. Míg az előbbi iskolába tartozó elméletek a közönséget passzív és az üzeneteket kritikátlanul befogadó homogén masszaként képzelték el, az utóbbiba tartozók a közönségnek az üzenetek dekódolásában játszott aktív és kritikus szerepét, a közönség heterogenitását, az egyes egyének eltérő értelmezési stratégiáit hangsúlyozzák. Míg az előbbi iskola

hívei szívesebben beszélnek a befogadók passzív hozzáállását és kiszolgáltatottságát sugalló „médiafogyasztásról”, az utóbbi hívei inkább a közönség autonómiáját és tudatos választását hangsúlyozó „médiahasználat” kifejezést használják
Az egyes médiahatás- és befogadáselméleteket az alábbi táblázat összegzi:

A legfontosabb médiahatás- és befogadáselméletek:

Direkthatás-elméletek	**Korlátozotthatás-elméletek**
lövedékelmélet (Lasswell, 1927)	kétlépcsős hatásmodell (Lazarsfeld et al., 1944)
kultivációs elmélet (Gerbner, 1969)	szelektívészlelés-elmélet (Klapper, 1960)
hallgatásispirál-elmélet (Noëlle-Neumann, 1974)	napirendelmélet (McCombs és Shaw, 1972)
*framing*elmélet (Herman és Chomsky, 1988)	használat és kielégülés-modell (Blumler és Katz, 1974)
	kódolás-dekódolás-modell (Hall, 1980)
	performatívhatás-modell (Dayan és Katz, 1992)

A fent leírt kutatásokat összegezve azt mondhatjuk, hogy a médiának az emberek gondolkodására és viselkedésére gyakorolt hatásának mértéke és iránya megjósolhatatlan – ám az biztos, hogy ez a hatás nem nagy, nem közvetlen és nem egyirányú.
Annak, hogy a média csak korlátozott mértékben és áttételesen képes befolyásolni a közönséget, az egyik oka az, hogy a modern demokráciákban a média csak egy az embereket befolyásoló számos tényező között (ott van mellette egyebek között a család, az iskola és az egyház). A különböző szocializációs ágensek különböző nézeteket közvetítenek és együtt hatnak az emberekre, e hatások között pedig a média hatását nem lehet elkülöníteni a többitől – már csak azért sem, mert a különböző társadalmi hatások a médiát is folyamatosan alakítják. A másik oka az, hogy a mai, sokcsatornás és sokszínű médiapiacon nem beszélhetünk egységes médialátképről: a különböző médiumok sokszor egymásével is szöges ellentétben álló üzeneteket fogalmaznak meg. A médiának az emberekre gyakorolt hatásáról a kutatók legfeljebb azt merik kijelenteni, „bizonyos médiumok bizonyos üzenetei bizonyos időkben bizonyos hatást gyakorolnak a közönség bizonyos részére”
A média és a közönség viszonya, egymásra gyakorolt hatása olyan összetett, hogy mindeddig nem sikerült egyetlen modellel meggyőzően leírni. A legtöbb említett kutatásról az is elmondható, hogy empirikus eredményeit szelektíven értékelte, azaz csak azokat az adatokat vette figyelembe, amelyek alátámasztották kiinduló hipotézisét. Így a kapott eredmények szükségszerűen egyoldalúak lettek, a különböző „iskolákba” tartozó kutatások eredményei pedig gyakran ellentmondanak egymásnak.

7.2. Tananyagegység

7.2.1.	Megnevezése	Biztonságos internethasználat

Adathalászat
Az adathalász támadás során a támadó megpróbál rávenni bennünket, hogy email-ben vagy egy közösségi oldalon keresztül érkezett üzenetben lévő hivatkozásra kattintva megnyissunk egy weboldalt vagy egy csatolt dokumentumot. Amennyiben áldozatául esünk egy ilyen támadásnak, akkor azt kockázatjuk, hogy a személyes, bizalmas adataink bűnözők kezébe kerülnek, vagy kártékony kóddal fertőződik meg a számítógépünk. A kiberbűnözők keményen dolgoznak azért, hogy az általuk küldött levelek minél meggyőzőbbek legyenek. Például olyan levelet küldenek, amely úgy néz ki, mintha baráttól vagy olyan megbízható cégtől jött volna, amellyel amúgy is kapcsolatban állunk. Az ilyen levelek esetében email címet hamisítanak, vagy olyan logót tesznek a levélbe, amit a bankunk is használ, majd az ilyen hamis leveleket több millió embernek küldik el. Azt nem tudhatják, hogy ki sétál be a csapdába, de azt igen, hogy minél több potenciális áldozatot vesznek célba, annál nagyobb az esélye annak, hogy sikert érnek el. Az adathalász támadás a hálóval való halászatra hasonlít. Nem tudhatjuk, hogy milyen halat fogunk ki, de minél nagyobb hálóval próbálkozunk, annál több halat foghatunk ki. A támadóknak számos módjuk van arra, hogy elérjék, amit akarnak:
Információk begyűjtése: a támadók célja, hogy megszerezzék a személyes adatainkat (jelszavak, hitelkártya számok, banki adatok, stb.). Ennek érdekében egy olyan weboldalra mutató hivatkozást küldenek nekünk, ami megtévesztésig hasonlít egy általunk ismert weboldalhoz, ami azt kéri tőlünk, hogy adjuk meg a személyes adatainkat. Mivel azonban ez egy hamis weboldal, az összes beírt információnk közvetlenül a támadókhoz kerül.
Káros tartalomra mutató hivatkozás: a támadó célja, hogy átvegye az irányítást az áldozat rendszere felett. Ennek érdekében káros tartalomra mutató hivatkozást küld, ami az áldozatot egy olyan weboldalra viszi, amely – sikeres támadás esetén – az eszközön keresztül megfertőzheti a rendszerét.

Káros tartalmú csatolmány: a támadó célja – hasonlóan az előzőhöz – megfertőzni az áldozat eszközét, és átvenni felette az irányítást. A különbség az, hogy ebben az esetben a levélhez csatolt melléklet (pl. egy Word dokumentum) megnyitásakor hajtódik végre a támadás, aminek következtében megfertőződhet a számítógépünk.
Csaló email-ek: vannak olyan adathalász email-ek is, amelyeket csalók küldenek a potenciális áldozatoknak. Ezek a levelek azzal próbálnak átverni bennünket, hogy azt állítják, megnyertük a lottót, jótékonysági szervezetnek mutatják be magukat, és támogatást gyűjtenek, vagy éppen abban kérnek segítséget, hogy több millió dollárt kellene eljuttatni egyik helyről a másikra. A levelekre adott válasszal a csalók vagy előleget kérnének, vagy hozzáférést a bankszámlánkhoz, hogy így fosszanak ki bennünket.
Így védekezzünk!
Az emailek és üzenetek megnyitása és elolvasása az esetek túlnyomó többségében rendben van. Ahhoz, hogy az adathalász támadások működjenek, a bűnözőknek trükköket kell bevetniük, de ezeknek mindig van valami nyoma, így könnyen lelepleződhetnek:

- az üzenet olyan dolgot sugall, hogy azonnal cselekedni kell, mielőtt „valami rossz dolog” történik (pl. felfüggesztik a felhasználói fiókunkat). A támadó célja, hogy a siettetéssel hibát kövessünk el;
- ha kapunk egy email-t olyan csatolmánnyal, amire nem számítottunk, vagy a levél arra akar rávenni bennünket, hogy nyissuk meg a csatolmányt (pl. azzal, hogy még be nem jelentett elbocsátásokról van benne szó, munkatársak fizetési adatait tartalmazza, vagy hogy az adóhivatal vizsgálatot indított ellenünk);
- a nevünk helyett egy általános megszólítást tartalmaz („Kedves Ügyfelünk!”). A barátok és jellemzően a ügyfelek is a nevünkön szólítanak meg bennünket;
- az email bizalmas információt kér (pl. banki adatok, jelszavak);
- az üzenet azt állítja, hogy hivatalos szervezettől érkezett, de ennek ellenére feltűnően hibás nyelvtannal íródott, vagy pedig privát email címeket tartalmaz (@gmail.com, @freemail.hu);
- az üzenet furcsa vagy nem hivatalosnak látszó hivatkozást tartalmaz. Ilyen esetben vigyük az egérmutatót a hivatkozás fölé, és egy felugró kis ablakban látni fogjuk, hogy az kattintásra hová is vinne bennünket. Ha a levélben lévő hivatkozás és a felugró ablak URL címe nem ugyanaz, akkor ne kattintsunk rá! Mobil eszköz esetén, ha az ujjunkkal lenyomva tartjuk a hivatkozást, ugyanezt érhetjük el. Egy biztonságosabb megoldás, ha kimásoljuk vagy beírjuk a helyes hivatkozást a böngészőbe, és úgy nyitjuk meg;
- az üzenetet olyan embertől kaptuk, akit ugyan ismerünk, de a levél hangvétele és szóhasználata mégsem olyan, mintha az a személy lenne a valódi küldő. Ha gyanakszunk, akkor inkább hívjuk fel az illetőt, és kérdezzük meg, hogy valóban ő küldte-e a levelet! A kiberbűnözők könnyen tudnak olyan email-t készíteni, ami látszólag egy baráttól vagy munkatárstól érkezett.

Ha egy email vagy üzenet adathalász támadásnak tűnik, akkor egyszerűen töröljük! A legjobb védekezés a józan ész használata.

Mi az a káros szoftver?
Egyszerűen fogalmazva, a káros szoftver olyan számítógépes program, amellyel kárt lehet okozni. A kiberbűnözők azért telepítenek káros szoftvereket a számítógépekre és más eszközökre, hogy átvegyék azok irányítását vagy hozzáférjenek a rajtuk található tartalomhoz. Miután sikeresen telepítették a káros szoftvert, a támadóknak lehetőségük van megfigyelni, hogy milyen tevékenységeket hajtunk végre az Interneten, ellophatják a jelszavainkat vagy fájljainkat, esetleg felhasználhatják a rendszerünket arra, hogy másokat támadjanak rajtunk keresztül. Ezeken kívül esetleg képesek meggátolni abban is, hogy hozzáférjünk saját állományainkhoz, „váltságdíjat” követelve azért, hogy ismét használhassuk azokat.
Sok emberben él az a tévképzet, hogy a káros szoftverek csak a Windows rendszereket érintik. Bár a Windows széles körben használt operációs rendszer, és éppen ezért vonzó célpont, a káros szoftverek képesek megfertőzni bármilyen – ide értve a Mac rendszereket is – számítógépet, okostelefont vagy táblagépet. Minél több számítógépet és más eszközt fertőznek meg a kiberbűnözők, annál több pénzt tudnak szerezni. Éppen ezért mindenki – még mi is – potenciális célpontnak számít.

Ki készíti a káros szoftvereket?
A káros szoftvereket már régóta nem csak érdeklődő hobbiprogramozók és amatőr hacker-ek készítik, hanem a kiberbűnözők is beszálltak a játszmába. Az ő céljuk az, hogy pénzt szerezzenek azzal, hogy megfertőzik a számítógépünket vagy más hordozható eszközünket, majd ellopják az azokon található adatokat, spam-et küldjenek, esetleg szolgáltatás megtagadásos támadást indítsanak mások ellen, vagy akár megzsaroljanak bennünket. A káros szoftverek készítői széles skálán mozognak: a saját céljaikat követő emberektől a szervezett bűnözői csoportokig terjed, de akár kormányzati szervezetek is részt vehetnek ilyenekben. Akik manapság káros szoftvereket fejlesztenek, azoknak gyakran ez a teljes munkaidejüket kitöltő tevékenysége,
kimondottan ebből élnek. Gyakran előfordul az is, hogy a munkájuk „gyümölcsét” eladják más személyeknek vagy szervezeteknek, és akár támogatást és rendszeres frissítést is biztosítanak az „ügyfeleknek”.

Hogyan védekezzünk?

A védekezés legáltalánosabb lépése az, hogy telepítünk egy megbízható forrásból származó víruskereső programot. Ezeknek az alkalmazásoknak kimondottan az a feladata, hogy észleljék és megállítsák a káros szoftvereket. Azonban nem képesek megállítani minden káros szoftvert. A kiberbűnözők folyamatosan fejlesztik a saját programjaikat, hogy azok képesek legyenek elkerülni a víruskereső programok által felállított csapdákat. A másik oldalról nézve pedig a víruskereső alkalmazások gyártói is folyamatosan fejlesztik, és újabb képességekkel ruházzák fel saját terméküket annak érdekében, hogy minél több káros szoftvert legyenek képesek felismerni. Tulajdonképpen ez nem más, mint egy fegyverkezési verseny, ahol mindkét fél célja, hogy túljárjon az ellenfél eszén. Általában sajnos a rossz fiúk egy lépéssel előrébb járnak. Mivel a biztonságunk nem függhet kizárólag a víruskereső programokon, érdemes megtenni az alábbi lépéseket a saját védelmünk érdekében:

- A kiberbűnözők gyakran úgy fertőzik meg a számítógépeket, hogy a szoftverekben lévő sérülékenységeket használják ki. Minél frissebb szoftvereket használunk, annál kevesebb sérülékenységet tudnak kihasználni a támadók, így nehezebb dolguk van, amikor megpróbálják megfertőzni a rendszerünket. Ezért mindig gondoskodjunk arról, hogy az általunk használt operációs rendszeren, szoftverekben, hordozható eszközökön engedélyezve legyen az automatikus frissítés!
- A bűnözők gyakori módszere a mobil eszközök megfertőzésére, hogy készítenek egy hamis alkalmazást, amit az Interneten keresztül terjesztenek, és megpróbálják rávenni az embereket, hogy letöltsék és telepítsék azt. Éppen ezért csak megbízható online áruházakból töltsünk le bármilyen alkalmazást! Továbbá, akkor csak olyan alkalmazást töltsünk le, amely már régóta ismert, sokan letöltötték, és sok pozitív visszajelzést kapott!
- A számítógépet ne használjuk adminisztrátor vagy root felhasználóval, hanem egy ezekhez képest csökkentett jogosultságúval! Ezzel további védelmet szerezhetünk azáltal, hogy megelőzzünk bizonyos káros szoftvereket abban, hogy települjenek.
- Gyakori trükk, hogy a kiberbűnözők megpróbálják rávenni a felhasználót arra, hogy saját maga telepítsen káros szoftvert. Például egy valódinak látszó email-t küldenek, amelyben csatolmány vagy hivatkozás van. A levél úgy is kinézhet, mintha egy ismerőstől vagy akár egy banktól érkezett volna. De ha megnyitjuk a csatolmányt, vagy rákattintunk a hivatkozásra, akkor aktiváljuk a káros szoftvert, az pedig már bármit telepíthet a gépünkre. Amennyiben egy email sürgető üzenetet tartalmaz, zavaros, esetleg túl jónak tűnik ahhoz, hogy igaz legyen, akkor lehet, hogy egy támadás. Legyünk gyanakvóak! A józan eszünk a legjobb védelmi eszköz.
- Rendszeresen készítsünk mentést a számítógépünkről, eszközünkről, illetve a fájljainkról, és a mentést vagy egy felhő alapú tárhelyen, vagy a számítógépről leválasztott, külső tárhelyen tartsuk! Ezzel a lépéssel megelőzhetjük a zsaroló, titkosító káros szoftverek által okozott károkat. A mentések rendkívül fontosak. Gyakran ez az utolsó mentsvárunk, ha egy fertőzés után kell helyreállítani a rendszerünket.

A káros szoftverek elleni legjobb védekezés az, ha naprakészen tartjuk a szoftvereinket, megbízható víruskereső programot telepítünk, odafigyelünk arra, hogy ne tudjanak becsapni bennünket, és ne tudják megfertőzni a rendszerünket.

Mit tegyünk, ha feltörtek?

Mindnyájunkat foglalkoztat a számítógépünk és mobil eszközeink biztonsága, amelynek érdekében természetesen lépéseket is teszünk. Azonban nem számít, hogy milyen biztonságosan használjuk a technológiát, előbb vagy utóbb mindenkit elérhet a végzet, amikor „feltörik” az eszközünket.

Gyanús jelek

Általában nem könnyű felismerni, ha valaki sikeresen feltörte a gépünket, mivel ennek felismerésére gyakran nincs kézzel fogható bizonyíték. Viszont a támadók számos nyomot hagynak maguk után, amelyeket indikátoroknak szokás nevezni. Minél több gyanús jelet észlelünk, annál valószínűbb, hogy feltörték azt.

- A víruskereső program jelzi, hogy a rendszer fertőzött, különösen akkor, ha azt mondja, nem tudja eltávolítani vagy karanténba helyezni a gyanús fájlokat.
- A böngésző kezdőoldala váratlanul megváltozott, vagy olyan oldalt nyit meg, amit nem akarunk.
- Olyan új felhasználói fiók van a számítógépen, amit nem mi hoztunk létre, vagy olyan programok futnak, amit nem mi telepítettünk.
- Az alkalmazások vagy akár a számítógép folyamatosan összeomlik, újraindul, ismeretlen alkalmazások ikonjai jelennek meg, vagy furcsa ablakok ugranak fel.
- Egy program engedélyt kér arra, hogy módosítást végezzen el a számítógépen, bár nem telepítettünk vagy frissítettünk semmit.
- A helyes jelszóval nem tudunk bejelentkezni a rendszerünkbe vagy egy online fiókba.
- Barátok kérdezik, hogy miért küldünk nekik kéretlen leveleket, amikor biztosak vagyunk abban, hogy semmit nem küldtünk.
- A mobil eszközünk engedély nélkül küld emelt szintű számra SMS üzenetet.

– A mobil eszközünk hirtelen minden magyarázat nélkül sok adatot forgalmaz, vagy gyorsan lemeríti az akkumulátort.

Mit tehetünk?
Amennyiben úgy gondoljuk, hogy feltörték a rendszerünket, akkor a minél gyorsabb reakció a legjobb lépés. Ha a szóban forgó eszközt az iskola biztosította, vagy munka céljára van fenntartva, akkor ne akarjuk mi magunk megoldani a problémát. Nem csak azért, mert több kárt okozhatunk, mint hasznot, hanem azért is, mert olyan értékes bizonyítékokat tüntethetünk el, amelyek segíthetik a nyomozást. Ehelyett inkább azonnal vegyük fel a kapcsolatot a rendszergazdával. Amennyiben nem lehetséges felvenni a kapcsolatot, akkor a kérdéses eszközt válasszuk le a hálózatról, kapcsoljuk ki (esetleg tegyük alvó vagy hibernált módba). Még ha nem is vagyunk biztosak abban, hogy feltörték a gépünket, akkor is jelentsük az esetet! Amennyiben a készülék a saját tulajdonunk, akkor az alábbi lépéseket javasoljuk megtenni:
Jelszóváltoztatás: nem csak az adott számítógép vagy mobil eszköz jelszavát kell ilyenkor lecserélni, hanem minden online felhasználói fiókét is, és ezt ne a feltört számítógépről végezzük el, hanem egy olyan másikról, amely esetében biztosak lehetünk abban, hogy elég biztonságos ehhez a művelethez.
Víruskereső program: ha a szoftver tájékoztat bennünket arról, hogy fertőzött fájlt talált, kövessük a tanácsait, ami általában a fájl karanténba helyezése, megtisztítása vagy törlése. A víruskereső programok rendszerint internetes hivatkozásokat is ajánlanak, ahol többet is megtudhatunk a szóban forgó káros szoftverről. Ha kétségünk van tegyük karanténba a fájlt! Ha ez nem lehetséges, akkor töröljük!
Újratelepítés: ha nem tudjuk kijavítani a fertőzés okozta károkat vagy ha teljesen biztosra akarunk menni, hogy semmilyen káros szoftver sem marad a rendszerünkön, akkor egy biztosabb megoldás az újratelepítés. Számítógép esetén kövessük a gyártó utasításait! A legtöbb esetben beépített szolgáltatások vannak a teljes újratelepítésre. Abban az esetben, ha ezek a lehetőségek nem állnak rendelkezésre (sérült, fertőzött, stb.), akkor vegyük fel a kapcsolatot a gyártóval, vagy látogassuk meg a weboldalukat! Soha ne telepítsük a rendszert egy korábbi biztonsági másolatból, mert az olyan sérülékenységeket tartalmazhat, amelyeken keresztül a támadó már sikeresen megfertőzte a rendszert. A biztonsági mentéseket csak az adatok helyreállítására használjuk! A mobil eszközök esetén kövessük a készülék gyártójának vagy a szolgáltatónak az utasításait, amiket megtalálhatunk a weboldalukon. A legtöbb esetben ez annyit jelent, hogy visszaállítjuk az eredeti gyári beállításokat. Amennyiben nem érezzük eléggé felkészültnek magunkat ehhez, vegyük igénybe szakértő segítségét! Amennyiben a számítógép vagy mobil eszköz már régi darab, lehet, hogy jobban járunk egy új vásárlásával. Végezetül pedig, ha sikeresen újratelepítettük az eszközt, kapcsoljuk be az automatikus frissítést, hogy mindig naprakészen tudjuk tartani.
• **Biztonsági mentés**: a védekezés legfontosabb lépése a rendszeres biztonsági mentés készítése, amely minél gyakoribb, annál jobb. Vannak olyan megoldások, amelyek akár óránként képesek menteni az új vagy megváltozott fájlokat. Függetlenül attól, hogy milyen megoldást veszünk igénybe, rendszeresen ellenőrizzük, hogy képesek vagyunk visszaállítani a mentésből az adatokat. Elég gyakran a biztonsági mentések visszaállítása az egyetlen mód, hogy egy betörés után helyreállítsuk a rendszert.
• **Hatóság értesítése**: ha úgy érezzük, hogy bármilyen módon fenyegetve vagyunk, értesítsük a rendőrséget!

Titkosítás
Mit nevezünk titkosításnak?
Mindannyian hallhattuk már azt a kifejezést, hogy titkosítás, illetve azt is, hogy ennek segítségével hogyan kellene megvédenünk magunkat és adatainkat. Azonban a titkosítás nem biztos, hogy mindenki számára egyértelmű, és tisztában kell lennünk a technológia lehetőségeivel és határaival. A mostani hírlevelünkben egyszerű kifejezésekkel mutatjuk be, hogy mi az a titkosítás, hogyan véd meg bennünket, és hogyan használhatjuk megfelelően.
Hatalmas mennyiségű személyes információt tárolunk a különböző eszközeinken dokumentumok, képek, email-ek formájában. Ha volt már példa arra, hogy elhagytuk vagy ellopták a mobil eszközünket, akkor az összes személyes információnkat megszerezhették azok, akik hozzáfértek a készülékhez. Ráadásul akár az elvégzett online banki műveletek vagy webshop-os vásárlások bizalmas információi is – mint például a bankszámla vagy bankkártyaszám is – illetéktelen kézbe kerülhet. A titkosítás segíthet az ilyen esetekben azzal, hogy idegenek nem tudják elolvasni vagy módosítani az információkat.
A titkosítást már évezredek óta használjuk. A ma használatos módszerek már nagyon kifinomultak, de végeredményben ugyanazt a célt szolgálják – üzenetet küldeni egyik helyről a másikra, miközben biztosak lehetünk abban, hogy csak az tudja elolvasni, akinek eredetileg is szántuk. A nem titkosított információt egyszerű szövegnek, más néven „plain-text”-nek nevezzük. Ez azt jelenti, hogy bárki könnyedén hozzáférhet, és el tudja olvasni. A titkosítás ezt az egyszerű szöveget átalakítja egy nem olvasható formára, amit titkosított szövegnek, más néven „cipher-text”-nek hívunk. A manapság használt titkosítások összetett matematikai műveleteket és egy egyedi kulcsot használnak a titkosított szövegek előállításához. A kulcs az, ami „nyitja” vagy „zárja” a titkosítással védett adatot, ez pedig a legtöbb esetben egy jelszó vagy jelmondat.
Mire használhatjuk a titkosítást?

Alapvetően kétféle információt kell titkosítással védeni: azt, amit a telefonon tárolunk, illetve azt, ami épp úton van egyik pontból a másikba (például üzenet küldünk vagy épp fogadunk).

A mobil eszközön tárolt adatok titkosítása életbevágó arra az esetre, ha elvesztenénk vagy ellopnák tőlünk a készüléket. A ma használatos eszközökön már hatalmas mennyiségű személyes és más bizalmas információ gyűlhet össze, viszont nagyon könnyű elveszíteni. Ezen felül más típusú hordozható eszközök (pendrive, külső merevlemez) is tartalmazhatnak olyan információkat, amiket nem szeretnénk mások kezében látni. A teljes lemeztitkosítás (Full Disk Encryption - FDE) egy széles körben használt titkosítási technológia, amely a teljes merevlemezt titkosítja. Ez azt jelenti, hogy minden automatikusan titkosításra kerül a rendszeren, tehát nem kell nekünk dönteni arról, hogy mi legyen, és mi ne legyen titkosítva. Manapság a számítógépek többsége már teljes mértékben támogatja a teljes lemeztitkosítást, bár azt még nekünk kell eldöntenünk, hogy be legyen-e kapcsolva. A Mac gépeken ezt FileVault-nak, a Windows-os rendszereken pedig Bitlocker-nek vagy eszköztitkosításnak (Device Encryption) nevezik. A legtöbb mobil eszköz szintén támogatja az FDE-t. Az iOS és iPad készülékek automatikusan bekapcsolják, amint első alkalommal beállítjuk a jelszavas védelmet. Az Android 6-os verziójától (Marshmallow) kezdődően a Google megköveteli az FDE bekapcsolását, amennyiben a készülék hardvere teljesíti a minimum elvárásokat.
Az információ akkor is veszélyben van, amikor elküldjük valahova, így amennyiben nincs titkosítva, könnyedén le lehet hallgatni, vagy akár módosítani is lehet. Ezért szükséges titkosítani minden bizalmas adatot és kommunikációt. Az online adatok titkosításának leggyakoribb módszere a HTTPS, ami azt jelenti, hogy minden adat, ami a böngészőnk és a weboldal között halad, az titkosításra kerül. Ha egy zárt lakat ikont látunk a https:// mellett, esetleg az egész címsor (ahova az URL-t írjuk) zöldre vált, akkor titkosított adatkapcsolat jött létre. Egy másik példa lehet, ha email-t küldünk vagy fogadunk. A legtöbb levelezőprogramnak megvan a képessége a titkosításra, de lehet, hogy engedélyeznünk kell azt. Vagy például ott vannak a chat alkalmazások, mint az iMessage, Wickr, Signal, WhatsApp vagy Telegram. Az ilyen alkalmazások is képesek arra, hogy a két végpont közti adatátvitelt titkosítsák, így harmadik fél nem képes hozzáférni ahhoz, vagyis csak a küldő és a fogadó képes elolvasni az üzeneteket.

Csináljuk jól!

Annak érdekében, hogy valóban jól működő titkosítást használjunk, érdemes betartani az alábbi szempontokat: A titkosítás pontosan olyan erős, mint a használt kulcs. Ha valaki kitalálja vagy megszerzi a kulcsunkat, hozzá fog férni minden adatunkhoz. Védjük meg a kulcsot! Ha jelszót használunk, akkor az legyen kellően erős és egyedi! Minél hosszabb a jelszó, a támadónak annál több időbe kerül feltörnie azt. Azonban ha elfelejtjük a jelszót, akkor többé nem fogunk hozzáférni a saját adatainkhoz. Használjunk jelszókezelő programot, a jelszavak biztonságos tárolásához.

• A titkosítás erőssége függ magától az eszköz biztonságosságától is. Ha egy támadó feltöri, vagy káros szoftverrel fertőzi meg az eszközt, akkor lehetősége nyílik megkerülni a titkosítást. Ezért nagyon fontos, hogy megtegyük az olyan megfelelő lépéseket a készülék biztonságossá tételéhez, mint például a víruskereső program és erős jelszó használata, valamint az eszköz folyamatos karbantartása, frissítése.

• Manapság már sok mobil vagy számítógépes alkalmazás tudja használni a modern titkosítási módszereket az adatok és a kommunikáció védelme érdekében. Amennyiben az általunk használtak nem képesek erre, érdemes alternatív megoldások után kutatni.

A biztonság megőrzése négy lépésben

Áttekintés

A technológia nemcsak egyre fontosabb szerepet tölt be az életünkben, hanem egyre bonyolultabbá is válik. Figyelembe véve a technológia fejlődési sebességét, nincs könnyű dolgunk akkor, ha naprakészek akarunk lenni biztonsági szempontból. Úgy tűnik, hogy mindig jönnek újabb és újabb útmutatók, tanácsok, amelyek megmondják, hogy mit kellene, és mit nem kellene tennünk. Bár a részletek változnak, az internetes biztonság alapjai tulajdonképpen ugyanazok, mint korábban. Függetlenül attól, hogy milyen technológiát használunk, vagy éppen hol vagyunk, javasolt az alábbi négy fontos lépés megtétele.

1. **Mi, mint felhasználók**: az első és legfontosabb, hogy mindig észben tartsuk, a technológia önmagában nem fog megvédeni bennünket, a támadók mindig találnak egy egyszerű módszert arra, hogy kijátsszák a biztonsági megoldásokat. Ha meg akarják szerezni a jelszavunkat vagy a hitelkártyaszámunkat, akkor különféle egyszerű trükkökkel el fogják érni, hogy mi magunk adjuk meg nekik. Például kapunk egy telefonhívást valakitől, aki azt állítja, hogy a Microsoft technikusa és úgy látja, hogy fertőzött a számítógépünk. A valóságban egy kiberbűnözőről van szó, aki így akar hozzáférést szerezni a rendszerünkhöz. Vagy ha kapunk egy email-t, amelyben azt állítják, hogy a megrendelt csomagunkat nem tudják kiszállítani, és ezért kattintsunk egy hivatkozásra, ahol meg tudjuk adni a címünket. Ezzel szemben a link egy hamis weboldalra vezet minket, amin keresztül káros szoftverek segítségével fel tudják törni a számítógépünket. A zsarolóvírusok és vezetői átverések is így kezdődnek. Végső soron a támadások elleni legjobb védelem mi magunk vagyunk. Legyünk óvatosak, használjuk a józan eszünket, és így felismerhetjük a legtöbb támadást.

2. **Jelszavak**: a védekezés következő lépése az, hogy egyedi, erős jelszót válasszunk minden egyes Internetre kapcsolódó eszköznek, online fióknak és alkalmazásnak. Nagyon fontos, hogy erős és egyedi jelszó legyen! Az erős azt jelenti, hogy a hacker-ek vagy az automatikus programjaik ne tudják könnyen megfejteni. Elegünk van már a bonyolult jelszavakból, amiket nehéz megjegyezni és beírni? Próbáljuk ki inkább a jelmondatokat. Egyetlen szóból álló jelszó helyett használjunk több szóból állót, könnyen megjegyezhető mondatot, mint pl. “Hol van a kávém?”. Minél hosszabb egy jelmondat, annál erősebb. Az egyedi azt jelenti, hogy minden eszközt és online fiókot saját jelszóval védjük. Ez azt jelenti, hogy ha valaki megszerzi a jelszavunkat, akkor más internetes szolgáltatások és eszközök nem kerülnek veszélybe. Nem emlékszel az erős, egyedi jelszavakra? Nem kell aggódni, néha mi sem. Ezért javasolt, hogy mindenki használjon egy jelszókezelő programot, amely képes titkosított formában tárolni a mobil eszközökön vagy számítógépen használt online fiókok jelszavait.
   Végezetül pedig mindig kapcsoljuk be a kétlépcsős hitelesítést minden olyan felhasználói fiókhoz, amely erre lehetőséget ad. A jelszavak egyedül már nem elegendőek az online fiókjaink védelmére, valami erősebbre van szükség, mint pl. a képlépcsős hitelesítés. Szükség van a jelszavaink használatára, de mindamellett egy második lépcsőt is igényel, ami lehet valami személyes tulajdonság (biometria), valami birtoklás alapú (mint pl. egy okostelefonra küldött kód vagy a telefonon lévő kódgeneráló alkalmazás). Engedélyezzük ezt az opciót minden egyes fióknál, ahol elérhető, még a jelszókezelő programnál is. A kétlépcsős hitelesítés valószínűleg az egyetlen és legfontosabb lépés, amit biztonságunk érdekében megléphetünk, és használata sokkal egyszerűbb, mint gondolnánk.

3. **Frissítések**: mindig legyünk naprakészek, telepítsük a legfrissebb operációsrendszer frissítéseket, a legújabb alkalmazásokat minden számítógépre, mobil eszközre vagy bármire, amivel csatlakozunk az Internetre! A kiberbűnözők folyamatosan keresik az aktuálisan használt technológiákban lévő sebezhetőségeket. Ha találnak egy sérülékenységet, akkor speciális programok segítségével kihasználják azokat, hogy feltörjék az eszközeinket, bármilyen technológiát is használjunk. Eközben a szoftvergyártók is folyamatosan dolgoznak azon, hogy az ismertté vált sérülékenységeket kijavítsák, majd ezeket frissítések formájában nyilvánosságra hozzák. Azzal, hogy mindig telepítjük a szoftvergyártók által készített javításokat, megnehezítjük a kiberbűnözők a dolgát, hogy betörjenek a számítógépünkbe. Ennek érdekében - amikor lehetőségünk van rá - kapcsoljuk be az automatikus frissítést. Ezt a szabályt ne csak a számítógép és mobil készülék esetén tartsuk szem előtt, hanem minden olyan eszköz esetén, amely kapcsolódik az Internetre – TV, baba monitor, otthoni router, játékkonzol, vagy akár az autónk. Ha a számítógépünk operációs rendszere, mobil eszközünk, vagy egy általunk használt technológia már nem támogatott és nem érhető el hozzá új frissítés, javasolt olyan új verzió beszerzése, amin van támogatás.

4. **Backups**: annak ellenére, hogy megteszünk minden óvintézkedést, előfordulhat, hogy mégis feltörik valamelyik eszközünket vagy fiókunkat. Az ilyen esetekben csak akkor lehetünk teljesen biztosak abban, hogy megszabadultunk a káros szoftver okozta fertőzéstől, ha teljesen töröljük az eszközön lévő rendszert, és újratelepítjük azt. Ha például a támadó megakadályozott bennünket abban, hogy hozzáférjünk a személyes állományainkhoz, képeinkhez, dokumentumainkhoz, stb., akkor az egyetlen lehetőségünk az, hogy egy korábbi biztonsági mentésből helyreállítjuk ezeket. Azért, hogy egy hasonló esetben cselekedni tudjunk, nagyon fontos, hogy rendszeresen készítsünk biztonsági mentést a személyes adatainkról, illetve hogy ellenőrizzük azt is, hogy a mentésből helyre tudjuk állítani azokat. Az operációs rendszerek és mobil eszközök többsége támogatja az automatikus mentést. Továbbá, javasolt, hogy biztonsági mentéseinket a felhőben vagy offline tároljuk, védve ezzel a kiberbűnözőktől.

7.3. Tananyagegység

7.3.1.	Megnevezése	Valós vs digitális/ál identitás

Ahogy eluralkodott a tömegkommunikáció, a személymarketing a profik kezébe került. A hollywoodi sztároknak megvannak a maguk sajtóügynökei, a politikai jelölteknek a reklámügynökségeik, és így tovább” (Kotler-Levy, [1969] 2012: 262). Az 1969-ben leírt gondolatok még az aszimmetrikus tömegkommunikációs viszonyokat tételezték fel, ahol a nevezett ismert személyek/közszereplők a nyilvánosság előtt építhették/menedzselhették identitásukat. Ehhez képest az internet, ezen belül is world wide web, s leginkább a közösségi média megjelenésével magunk is márkává váltunk (Schawbel, [2009] 2012) abban az értelemben, hogy mindenki egy ponton a nyilvánosság, a nyilvánosan elérhető, lenyomozható, megkereshető, megfigyelhető adatkészlet részévé válik – még akkor is, ha nem ez volt az eredeti szándéka.

Ha egy márka, egy vállalat vagy egy személy nem érhető el online, felmerül, hogy nem is létezik. Hitelessége, megbízhatósága, ellenőrizhetősége válhat kérdésessé – és elveszítheti a lehetőséget arra, hogy újabb üzleti vagy emberi kapcsolatokat létesítsen.

Másik oldalról viszont az a kérdés, hogy láthatatlanok maradhatunk-e? Azaz vannak-e olyan cégek vagy személyek, akik saját döntéssel maradnak háttérben, kik azok, akik szándékosan nem hagynak digitális lábnyomokat, és kik azok, akiknek például egy munkaadó szabályozza a láthatóság mértékét. Például azért, mert a cél a kontroll, illetve a biztonság.
A weben élünk, alkotunk, tájékozódunk és tájékoztatunk. Itt lehet megfigyelni másokat és itt figyelnek meg minket mások. Az internetes nyilvánosság felteszi azt az alapvető kérdést, hogy mennyire akarunk láthatóak lenni, milyen közösségekhez akarunk tartozni, és melyekhez nem, mit szeretnénk mondani magunkról online és mit nem.
Végeredményben tehát azzal is üzenünk, ha online láthatóak vagyunk és azzal is, ha nem.

Mik azok a hamis profilok?
Hamis profilt hoz létre egy közösségi oldalon az, aki nem a saját nevében, hanem valaki más személyiségével visszaélve vagy egy kitalált személy profiljával regisztrálja magát. Egy ilyen fiktív személyiség eszköz lehet például online behálózáshoz, hiszen kitalált tulajdonságaival könnyebben elnyerheti a gyanútlan áldozat bizalmát és homályba burkolhatja az elkövető kilétét. Ma akár 150 millió visszaélésekre alkalmas, hamis profil is létezhet az interneten. A nagy szolgáltatók aktívan küzdenek a jelenség ellen.
Hamis a profil vagy egy fiók, ha azzal valaki nem a hiteles személyazonosságát képviseli, hanem egy kitalált személyre vagy egy híresség re hivatkozik. Amikor például egy ismert énekest vagy színészt próbálunk megkeresni egy közösségi oldalon, láthatjuk, hogy több, első látásra az általunk keresett személyhez köthető profil is létezik, és nehezen eldönthető, hogy valójában melyik az eredeti.
Aki egy létező személy nevében regisztrál profilt a közösségi médiában, komoly jogkövetkezményekkel is számolhat, hiszen egy másik ember személyiségével él vissza, megsértve annak személyiségi jogait. Polgári jogi értelemben ez a becsülethez és jó hírnévhez való jog megsértését és a képmásával való visszaélést jelentheti. Az elkövetőt eltilthatják a további jogsértéstől és sérelemdíj megfizetésére is kötelezhetik. Büntetőjogi szankciókra is sor kerülhet, ha a hamis profilon keresztül bűncselekményt követtek el, például személyes adatokkal éltek vissza.
Amikor a hamis profil a behálózás (grooming) eszköze
A kitalált személyekre vonatkozó, hamis profilok létrehozói sokszor online behálózás céljából teremtenek maguknak egy virtuális személyiséget. Az online behálózás céljából alkotott hamis profilokkal a létrehozó elkövethet zaklatást, visszaélhet az áldozat személyes adataival, sőt, gyermekektől kicsalt szexuális felvételekkel a gyermekpornográfia bűncselekménye is megvalósulhat.
A Facebook szabályzata is tiltja a nem valós adatokkal létrehozott profilokat. Aki hamis profilba ütközik az oldalon, így jelentheti:
https://hu-hu.facebook.com/help/306643639690823?helpref=related
Instagramon is:
https://help.instagram.com/446663175382270
A Tumblr, a Twitter és a Snapchat is fogadja a visszaélésekkel kapcsolatos bejelentéseket:
https://www.tumblr.com/abuse/confusion
https://support.twitter.com/forms/impersonation
https://support.snapchat.com/en-US/i-need-help

7.4. Tananyagegység

7.4.1.	Megnevezése	Forráshasználat és kritika: hírek és álhírek megkülönböztetése

Álhírek / fake news – nagyjából két éve, az amerikai elnökválasztási kampány alatt került (ismét) fókuszba a fogalom, holott a műfaj a nyomtatott sajtóval egyidős. A szándékos félretájékoztatást szolgáló hamis hírek a villámgyors online kommunikáció és közösségi média korában nagyon gyorsan okozhatnak hatalmas károkat. Rajtunk is múlik, hogy minek dőlünk be, de az EU is igyekszik tisztítani a helyzetet és szabályozni ezt a különösen nehéz területet.

El sem olvassuk, de megosztjuk
Manapság az európaiak közel fele (46%), a magyarok pedig több mint fele elsősorban a közösségi médiában olvassa és onnan osztja meg a híreket – általában anélkül, hogy leellenőrizné a forrásukat. Riasztó, hogy felmérések szerint tízből hat (!) hírt elolvasás nélkül osztanak meg. Ez különösen nagy probléma a politikai propaganda és a gyűlöletbeszéd esetében, mert a hamis információk és az álhírek így egyre könnyebben és gyorsabban terjednek.

Motivációk a fake news mögött

A valódi hírnek tűnő félretájékoztatásnak és álhíreknek több célja is lehet. Egyik az, hogy manipulálják az olvasókat, például politikai céllal – ez történt például a 2016-os amerikai elnökválasztás idején is, amikor többen kattintottak a kampányokat övező hamis információ kra a Facebookon, mint az igazi hírekre. Egyesek szerint már egy „posztfaktuális", azaz igazság utáni korbanélünk („post-truth era": az oxfordi angol szótár 2016-ban ezt választotta az év szavának). Ez annyit jelent, hogy a közvélemény formálásában a tények másodlagosak, és az érzelmek és személyes meggyőződések számítanak igazán.
A kamuhírek születhetnek szimplán profitszerzési szándékkal is: a szenzációhajhász („clickbait") címek és leadek célja, hogy minél több kattintást vonzanak adott oldalra, és így minél több olvasót szállítsanak különböző hirdetéseknek.
Mindezek egyértelműen káros hatással járnak, megtévesztik az olvasókat, amelynek nagyon komoly – akár pénzügyi, egészségügyi, pszichikai – következményei is lehetnek. Éppen ezért az álhírekkel szemben mindenképpen fel kell lépni, de úgy, hogy közben a fontos alapvető szabadságjogok – a sajtó- és szólásszabadság, a médiapluralizmus – ne sérüljenek.

Legyünk résen!

Az álhírek gyors terjedése mögött gyakran az áll, hogy sokan, akik az interneten olvasnak híreket, nincsenek tisztában az információk ellenőrzésének fő szabályaival, eszközeivel és lehetőségeivel. Legyetek résen!

KÜZDELEM AZ ÁLHÍREK ELLEN

Hogyan ismerheted fel az álhíreket (fake news)?

europapont
facebook.com/europapont
europapont.blog.hu

MEGBÍZHATÓ A FORRÁS?

Nézd meg az oldal impresszumát, és gyanakodj, ha híroldalként nem .hu a végződése! Ellenőrizd a hírt más forrásból is! Gyanús, ha szenzációt ígér, vagy ha az oldal neve hasonlít valamely ismert híroldaléhoz.

ELLENŐRIZD A SZERZŐT!

Nézd meg, ki jegyzi a cikket – ha névtelen, az gyanús. Hiteles? Ha valódi újságíró írta, biztos megtalálod korábbi cikkeit.

NÉZZ UTÁNA A HIVATKOZÁSOKNAK!

Kattints rá a hivatkozásokra – győződj meg róla, hitelesek-e. Valódi szakértőtől származnak az idézetek? Anonim vagy nem beazonosítható szakértőnél gyanakodj!

ELLENŐRIZD A DÁTUMOT!

Győződj meg róla, hogy a cikk aktuális, és nem egy korábbi hírt használnak fel újra a közösségi médiában. Korábbi negatív hírek ismételt megosztása felesleges riadalmat kelthet.

NEM EGY VICCOLDALT NÉZEL?

A valóság néha abszurdba hajlik – de azért gyanakodj, ha valami szokatlant olvasol hétköznapi témáról. Az oldal és a szerző ellenőrzése segíthet eldönteni, hogy szatirikus oldalról van-e szó.

NE ADD TOVÁBB GONDOLKODÁS NÉLKÜL!

Egy kutatás alapján tízből hat olvasó elolvasás nélkül megosztja a közösségi médiában megjelenő rövid híreket. Ne dőlj be a clickbait címeknek, mindig ellenőrizd a hírt, mielőtt továbbadod!

Készült: az International Federation of Library Associations and Institutions "How to spot fake news" összefoglalója, az Európai Parlament "Hogyan ismerjük fel az álhíreket" videója és az Álhírvadász oldal (alhirvadasz.hu) alapján.

további információ, álhírteszt:
www.alhirvadasz.hu
http://www.urbanlegends.hu/2018/01/megteveszto_atveros_magyar_oldalak_kamuhirek_lista_2018/

7.5. Tananyagegység

7.5.1.	Megnevezése	Darknet, becserkészés, cyberbullying, online predátorok, gyűlöletbeszéd

Mi van az internet alatt?
Egyrészt érdemes tisztázni az alapfogalmakat, amiket már sokan eleve összekevernek. Az "internet alatti internetnek" ugyanis két főbb szintjét lehet megkülönböztetni, amik teljesen másra valók. A felső szint az úgynevezett Deep Web, azaz Mély Internet: ez gyakorlatilag minden olyan adatot, oldalt és szolgáltatást jelent, amelyet nem indexelnek a keresők, nem talál meg közvetlenül a Google, vagy nem érhetjük el szimplán egy webcím begépelésével. Ezek azonban még nem feltétlenül illegális dolgok, ide tartozik például minden olyan fórum vagy közösségi tevékenység, amit csak regisztráció során érhetünk el, személyes fiók, privát felhőtárhely, céges fórumok és telephelyek közötti "privát internet-szeletek", virtuális irodák és még egy csomó egyéb.
Ami már tényleg a mélyben húzódik meg, az a Dark Web, azaz a Sötét Internet. Ez alapvetően egy olyan hálózatot jelent, amelyet a megfelelő módszerekkel teljesen anonim módon használhatunk, tehát bármi, amit olvasunk, megnézünk vagy akár létrehozunk, azt hatóságok, államok, vagy akár kutakodó ismerősök sem köthetik hozzánk.
A sötét interneten nem találunk valami.hu vagy bármimás.com jellegű webcímeket, hanem bonyolult kódsorok jelzik az oldalakat, a végződésük pedig mindig a .onion kiterjesztés. Igen, az onion hagymát jelent, és igazából ez a technológia a titkosítás alapjául szolgáló, sokrétegű megoldás miatt kapta a nevét. Érdemes tudni, hogy az .onion oldalakat, valamint a Tor által használt titkosítási algoritmust eddig még nem sikerült feltörnie senkinek, pedig dolgozik rajta mindenki mindenfelé. Különböző országok hatóságai értelemszerűen a bűnözés visszaszorítása miatt látnának bele szívesen a sötét netbe, míg vannak olyan országok, ahol a szólásszabadság elfojtása miatt menekülnek szószólók, illegális pártok, véleményvezérek a sötét web védelmébe. Oroszországban például teljesen legális, állami szinten kínálnak mesés vagyonokat annak, aki képes feltörni a Tor mögötti titkosítást és hozzáférést ad a kormánynak a másként gondolkodók személyéhez.

Hogyan történik az online behálózás?
Néha nem lehetünk biztosak abban, hogy akivel az interneten kapcsolatba kerültünk, valóban az-e, akinek mondja magát. Az online behálózás azt jelenti, hogy egy ismeretlen, gyakran egy felnőtt próbál – magát valaki másnak, például tizenévesnek kiadva – egy gyerek vagy fiatal bizalmába férkőzni, információkat kicsalni tőle, majd valahogy visszaélni hatalmi helyzetével. Mindez különböző fokozatokra, stratégiákra épül, hogy az érzelmileg elhanyagolt, bizonytalan gyermeket mielőbb megnyissa az elkövető felé. A legkiszolgáltatottabbak azok a gyermekek, akik bizonytalan körülmények között, stabil, szerető családi háttér nélkül élnek.
Amikor a gyerekek közösségi felületeken ismerkednek, akkor kitehetik magukat az online behálózás, becserkészés veszélyének is. Az esetek tanúsága szerint jellemzően egy magát kamasznak kiadó felnőtt próbál egy gyermek, fiatal bizalmába férkőzni, hogy személyes információkat csaljon ki tőle. A behálózó hatalmi helyzetbe kerül, amivel később visszaél. Követelhet pénzt, intim felvételeket, amelyeket ismét zsarolásra használhat, de személyes kapcsolatot, szexuális együttlétet is kezdeményezhet.
Ilyen helyzet – többek között – akkor alakulhat ki, amikor egy fiatal olyan személyt fogad el ismerőseként online, akivel valójában még soha nem találkozott, csak egy ismerős ismerősének látszik, vagy a profilja alapján rokonszenves, esetleg közös a hobbijuk, a kedvenc zenéjük.
A behálózás különböző fokozatokon keresztül valósul meg, sokszor tudatos stratégiára épül, amelyhez jellegzetes gesztusok, mondatok tartoznak. A behálózó figyel arra, hogy a beszélgetéseik bizalmasak és titkosak legyenek („Nyugodtan mondd el a legféltettebb titkaidat. Nem árulom el senkinek.”), igyekszik az áldozatról minél több olyan személyes információt megtudni („Hol szoktál bulizni?”, „Melyik suliba jársz?”), amelyek később még a hasznára lehetnek. Miután a gyermek bizalmába férkőzött, sokszor fenyegetőzik például a birtokába jutott felvételekkel („Ciki lesz, ha posztolok rólad képeket!”).
Az online behálózás során könnyen visszaélhetnek az áldozat személyes adataival, képmásával, de a zaklatás vagy a gyermekpornográfia is megvalósulhat. Ezek mind szabadságvesztéssel járó bűncselekmények.

Kik a leginkább kiszolgáltatottak?
A potenciális áldozatok azok a fiatalok, akik kevésbé médiatudatosak, érzelmileg elhanyagoltabbak, akiknek az életéből hiányzik legalább egy biztos kötődést nyújtó személy, mint például az állami gondozásban élő vagy a problémás családi hátterű, veszélyeztetett gyerekek. Az online behálózók azt a szükségletet használják ki, hogy ezek a gyermekek fokozottabban igénylik az odafigyelést és a törődést. Gondoskodást, barátságot vagy szerelmet hazudnak az áldozatnak, aki cserébe fokozatosan bevonódik az őt egyre inkább kihasználó kapcsolatba.

Bárki keveredik is ilyen bűnöző hálójába, ne szégyelljen segítséget kérni. Az elkövetővel folytatott csevegéseket, tőle kapott képeket érdemes elmenteni, hogy minden fontos információ a nyomozó hatóság rendelkezésére álljon. Mi magunk is sokat tehetünk az online biztonságunk érdekében, ha a közösségi oldalunkhoz való hozzáférést az alkalmazás biztonsági beállításaival korlátozzuk az idegenek előtt. A posztjainkat, képeinket is csak az ismerőseink számára tegyük láthatóvá, idegeneket lehetőleg zárjunk ki online kapcsolatainkból.

Gyűlöletbeszéd

Az online kommunikációt uraló nagy informatikai cégek közösen küzdenek a kirekesztő, sértő és gyűlöletet szító internetes kommunikáció ellen. A Google (YouTube), a Microsoft, a Twitter és a Facebook az Európai Bizottsággal együttműködve egy olyan megállapodást írt alá, amely alapul szolgálhat az ilyen ellenségeskedést gerjesztő online megnyilvánulások kezelésére.

Az online felületek remek lehetőséget nyújtanak arra, hogy egymástól távol élő emberek megosszák egymással véleményüket, vitázzanak, eszmét cseréljenek az őket érdeklő jelenségekről. Megvan ugyanakkor a veszélye is az internetes kommunikációnak: számos olyan fórum létezik, ahol – kihasználva a névtelenséget – az online csatornákat valaki vagy valami ellen irányuló ellenségeskedésre, gyűlöletkeltésre, uszításra vagy akár terrorista eszmék terjesztésére használják. Ez a jogellenes online gyűlöletbeszéd.

A szabad véleménynyilvánítás egy nagyon fontos alapjog, amellyel azonban bizonyos emberek vagy csoportok úgy is visszaélhetnek, hogy közben mások jogait, vagy akár létét fenyegetik. A közösségi média sajnálatos módon az egyik olyan eszköz, amelyet a terrorista csoportok a fiatalok radikalizálására, a rasszista csoportok pedig az erőszak és a gyűlölet terjesztésére használnak. Ez az, amelynek gátat kíván szabni az Európai Bizottság, és ebben nagyon fontos partnerei a legnagyobb online cégek. Gyűlöletbeszédnek és büntetendőnek minősül „*nyilvánosság előtt erőszakra vagy gyűlöletre uszítás faji, bőrszín szerinti, származás szerinti, vallás, meggyőződés, illetve nemzeti, etnikai hovatartozásuk alapján meghatározott személyek csoportjával vagy ilyen csoport valamely tagjával szemben*”.

Az informatikai vállalatok ezt az online térre vonatkoztatva nemrégiben **egy közös magatartási kódexet írtak alá**, amely alapján elkötelezik magukat, hogy:

- a gyűlöletbeszédre vonatkozó bejelentések többségét 24 órán belül felülvizsgálják, szükség esetén eltávolítják vagy hozzáférhetetlenné teszik ezen tartalmakat;
- belső eljárásokat alakítanak ki mindezek biztosítására;
- világosan kommunikálják a felhasználók felé, hogy platformjaikon mely viselkedések merítik ki a jogellenes gyűlöltbeszéd fogalmát;
- személyzetüket ennek megfelelően képzik.

Cyberbullying

A gyűlölködés, azaz a sértő, inzultáló vagy zaklató online viselkedés növekvő mértékben terjed. Sértő hozzászólások és klipek, módosított képek (úgynevezett mémek), a gyűlölködést promotáló játékok csak néhány megjelenési formáját jelentik annak a tartalomnak, amelyet a fiatalok maguk hoznak létre, és amellyel megsértik, bántják egymást. Az ilyen támadásnak kitett fiatalok sok esetben nem képesek érzelmileg feldolgozni az inzultust: a visszautasítottság és kitaszítottság érzete, búskomorság, önkritika és a védtelenség emóciói kerítik őket hatalmukba. A támadások szemtanújaként a fiatalok gyakran akaratlanul is növelik az áldozat fájdalmát azzal, hogy “lájkolják” vagy megosztják az ilyen zaklató jellegű tartalmat. Másfelől, a gúnyolódók sok esetben nincsenek is tudatában annak, mit miért tesznek – támadásuk mozgatórugója néha az irigység, az alacsony önértékelés, az online “hírnév” megszerzése, társaik elismerésének elnyerése, vagy egyszerűen csak az unalom. A (hibásan vélt) anonimitás érzete, és az, hogy nem szembesülnek az áldozatuk reakciójával gyakran olyan kijelentésekre vagy tettekre sarkallják őket, amelyeket a mindennapi életben nem tennének meg.

1. Mi a véleményed a gyűlölködők viselkedéséről? Mit gondolsz, miért cselekszenek így?

•irigység,
•a figyelem magára irányítása, népszerűség-hajhászás
•alacsony önértékelés – vágy arra, hogy másokat megalázva jobban érezze magát valaki
•képtelenség arra, hogy véleményét konstruktív módon fejezze ki
•unalom

2. Hogyan kéne az áldozatoknak viselkedniük egy ilyen helyzetben?

•Hagyjuk figyelmen kívül a hozzászólásokat – gyűlölködésre gyűlölködéssel válaszolni nem érdemes, mert csak eszkalálja a konfliktust
•Beszéljünk egy felnőttel a történtekről
•Ha van rá mód, töröljük a hozzászólást
•Húzzuk meg a vonalat és nevezzük nevén a szituációt, pl.: amit most teszel, az gyűlölködés, nem akarom, hogy ilyen stílusban írj nekem; megállítom a gyűlölködésedet, mert én ebben a stílusban nem válaszolok neked
•Jelentsük az esetet az oldal vagy portál adminjának
•Blokkoljuk a gyűlölködőt a profilunk hozzáférői közül

3. Milyen más módokon viselkedhetnének a gyűlölködők? •Fejezd ki a véleményed udvarias formában – hangsúlyozd, hogy csak a saját véleményed mondod, és fókuszálj a tárgyszerűségre, pl. játékstílus, csapatmunka, stratégia egy online játék esetén
•ne kommentálj

4. Mit kellene a szemtanúknak tenni?
•Ne lájkoljunk vagy osszunk meg sértő hozzászólásokat
•Ne válaszoljunk gyűlölködésre gyűlölködéssel
•Álljunk ellent, tehát írjunk a gyűlölködőnek, hogy amit tesz, az nem helyes
•Támogassuk az áldozatot
•Értesítsünk egy felnőttet
•Jelentsük a negatív, sértő hozzászólásokat az

Gyűlölködés elleni szabályok

1.Gondolkodj, mielőtt válaszolsz egy gyűlölködő kommentre. Ne hagyd, hogy az érzelmeid felülkerekedjenek rajtad, ne a pillanat hevében válaszolj.
2.Ha tényleg dühös vagy, írj egy választ, vegyél egy mély levegőt, és töröld ki.
3.Ne válaszolj agresszióra agresszióval – az agresszív válasz csak provokálja a gyűlölködőt, hogy folytassa a zaklatást.
4.Ne lájkolj és ossz meg gyűlölködő kommenteket – ezzel csak a terjesztésükben segítesz.
5.Ha lehetséges, töröld a gyűlölködő hozzászólásokat.
6.Ha gyűlölködést és a gyűlöletbeszédet tapasztalsz, jelentsd az oldal (fórum vagy közösségi oldal) adminisztrátorainak.
7.Nem minden kritika gyűlölködés. Tanuld meg megkülönböztetni a konstruktív kritikát a gyűlölködéstől.
8.Ha valami nem tetszik, vagy feldühít, fejezd ki érzelmeidet udvarias formában, ne gyűlölködéssel.
9.Sose hagyj fel azzal, amit teszel, gondolsz vagy mondasz a gyűlölködők miatt.
10.Ha úgy érzed, már nem tudod kezelni a gyűlölködőt, fordulj egy olyan felnőtthöz, akiben megbízol, vagy keresd meg a hazai Safer Internet konzorciumot! Itt a Kék Vonal Gyermekkrízis Alapítvány üzemeltet egy éjjel-nappal ingyen hívható telefont (116-111), illetve chat-szolgálatot (http://www.kek-vonal.hu/index.php/hu/bejelentkezes/login). Ezeken keresztül elmondhatod, hogy mi bánt, és ők tanácsokkal tudnak segíteni, hogy mitévő legyél!

A cyberbullying jelentése internetes megfélemlítés, zaklatás. Online térben, elektronikus eszközökön és különböző online, közösségi felületeken keresztül, szándékosan elkövetett cselekmény, amelynek célja az áldozat megszégyenítése és megalázása. Az ismételt elkövetés, ami a hagyományos zaklatásnak alapvető eleme, az online környezetben nem szükséges feltétel, itt akár egyetlen cselekmény elég a megfélemlítéshez: egy megosztással is pillanatok alatt eljuthat a lejáratő üzenet több száz emberhez. Jellemző, hogy az elkövető és az áldozat között az erőviszonyok kiegyensúlyozatlanok, az erősebb személy, az elkövető nyomást gyakorol a gyengébbre, az áldozatra. Az online anonimitásba vetett hit csak tovább erősíti ezt az egyenlőtlenséget.
Online megfélemlítés történik, ha az áldozatot a Facebookon kommentekben alázzák meg vagy kínos képet töltenek fel róla az engedélye nélkül, vagy az elkövető a saját blogján vagy vlogján szégyeníti meg. Az e-mailben kapott bántó, fenyegető üzenetek is online megfélemlítésnek számítanak.
Az áldozat számos joga sérül ilyen helyzetben, főként az emberi méltósághoz való joga és egyes személyiségi jogai. Büntető törvénykönyvünkben nincs önálló tényállás az online megfélemlítés szankcionálására, így a hagyományos, „offline" zaklatás (Btk. 222. § Zaklatás) tényállása áll legközelebb hozzá. Egyelőre az európai jogrendszerekben sem találkozhatunk önálló tényállásként az online megfélemlítéssel, a jogalkalmazók az ilyen cselekményt – többek között – a zaklatás, fenyegetés vagy becsületsértés tényállásai alapján ítélik meg, de alkottak már olyan tényállásokat is, amelyek figyelembe veszik a technológiai fejlődést.
Horvátországban bekerült a büntető törvénykönyvbe a gyermekkel szexuális kizsákmányolás céljából történő ismerkedés tényállása, amikor az elkövető egy 15. életévét be nem töltött személlyel online ismerkedik abból a

célból, hogy szexuális vágyait kielégítse. Csehország büntetőjoga pedig nevesíti a szexuális kizsákmányolási célú zsarolást: az elkövető szexuális cselekmény végzésére vagy ruhátlan felvétel készítésére kényszeríti az áldozatot, zsarolva őt egy – már a birtokában lévő – szexuális tartalmú képpel vagy videóval.
Az USA 22 tagállamában már léteznek olyan zaklatásellenes (antibullying) törvények, amelyek nevesítve is rendelkeznek a megfélemlítés online formáiról. Hosszú út vezetett idáig, a törvényalkotás legfőbb ösztönzői olyan tragikus esetek voltak, amelyekben fiatal emberek váltak annyira agresszív online megfélemlítés áldozataivá, hogy az öngyilkosságot látták az egyetlen kiútnak.

Miért kockázatos a szexting?
Szextingre akkor kerül sor, ha valaki saját magáról készített erotikus képet, videót vagy nyíltan szexuális tartalmú szöveges üzenetet küld ismerősének mobilon vagy az interneten keresztül. Könnyen megvalósítható és veszélyes jelenség, hiszen a küldő a meztelen képek sorsát a címzett kezébe adja. A visszaélések is hamar egymásra épülhetnek a méltóság sérelmétől a zaklatásig.
A szexting (eredetileg szex + texting, vagyis szexuális tartalmú sms-küldés) egy felhasználó által saját magáról készített szexuális tartalmú, provokatív, meztelen vagy félmeztelen képek, videók vagy szexuális felhívást tartalmazó üzenetek továbbítását jelenti, mobilhálózaton vagy az interneten. A képet küldő személy talán bele sem gondol a kockázatokba: pillanatok alatt bárkivel, akár a tágabb nyilvánossággal is megosztható a felvétel. Bár a küldő személy önként készítette és küldte el a képet, ahhoz viszont nem járult hozzá, hogy felhasználják, továbbítsák, megosszák a felvételt, például közzétegyék egy Facebookcsoport-beszélgetésben.
Ezekkel az intim felvételekkel nagyon könnyű visszaélni. Súlyosan sérül a küldő személy emberi méltósághoz való joga és a képmáshoz való joga, a képet mint különleges adatot nyilvánosságra hozó személy elkövetheti a személyes adattal való visszaélés vagy akár a gyermekpornográfia bűncselekményét is. A szexting következtében nyilvánosságot nyert fotók egy későbbi online megfélemlítés, zaklatás alapját is adhatják, sőt a készítő-szereplő akár folyamatos zsarolásához is felhasználhatóak. Így épülhetnek egymásra a visszaélések az enyhébbtől a legsúlyosabb sérelmekig.
A legegyszerűbben természetesen úgy védhetjük meg magunkat, ha tisztában vagyunk a szexting veszélyeivel, és egyáltalán nem küldünk ilyen jellegű felvételeket.

Hogyan kezelik a jogrendszerek a bosszúpornót?
A bosszúpornó azt jelenti, hogy valaki másokról készült szexuális tartalmú felvételeket tesz közzé az interneten, hogy megszégyenítse vagy bosszút álljon a felvételen szereplő személyen, személyeken. Ilyen tartalmakhoz már gyűjtőoldalakat is készítettek, remélve, hogy vagy a néző, vagy a megzsarolt áldozat fizetni fog. A jelenséget a jog sem nézi tétlenül, már hazánkban is került bíróság elé bosszúpornóhoz kapcsolódó ügy.
A bosszúpornó (angolul: revenge porn) gyakran egy szakítás után kel életre, amikor a pár egyik tagja bosszúból közzéteszi az interneten a korábbi közös, akár közös megegyezéssel készített, szexuális tartalmú videójukat vagy a másikról készített intim felvételeket, ekkor már az érintett hozzájárulása nélkül. Ezzel súlyosan sérti volt párja személyiségi jogait, emberi méltóságát.
Hazánkban nem önálló büntetőjogi kategória a bosszúpornó jelensége, de többféle kategóriában is megítélhető: személyes adattal való visszaélés, rágalmazás, szexuális kényszerítés, zsarolás vagy akár gyermekpornográfia is megvalósulhat benne.

A személyes adattól a rágalmazás minősített esetéig
A szexuális életre, szokásokra vonatkozó adatok személyes adatoknak minősülnek, azon belül is különleges adatoknak, így az azokkal történő visszaélés a büntetőjogba ütközik és akár két év szabadságvesztést is maga után vonhat.
Rágalmazás az, ha valakiről más előtt a becsület csorbítására alkalmas tényt állítanak, híresztelnek, ezért egy évig terjedő szabadságvesztés szabható ki. Minősített eset, ha az előbbieket aljas indokból vagy célból (ide sorolhatjuk a szerelemféltést is), nagy nyilvánosság előtt (például az interneten) vagy jelentős érdeksérelmet okozva követik el, ilyenkor két évig terjedő szabadságvesztés is lehet az ítélet. Az, amikor például valakinek a szexuális szokásairól osztanak meg felvételeket a beleegyezése nélkül, alkalmas lehet a becsület csorbítására, hiszen az emberi méltóságát támadják, derül ki a Kúria 21/2013. számú büntető elvi határozatból. A Kúria határozata bosszúpornó-ügyben: http://www.kuria-birosag.hu/hu/elvhat/212013-szamu-bunteto-elvi-hatarozat

Kényszerítéstől a zsarolásig
Szexuális kényszerítés kísérletévé akkor válik a bosszúpornó, amikor például valaki azzal fenyegeti a párját, hogy ha az elhagyja, közzéteszi a korábban készített szexuális felvételeket. Zsarolás bűncselekménye merül fel, ha a korábbi felvételeket a volt partner fizetség ellenében tartja vissza a közzétételtől.

18 éves kor alatt: gyermekpornográfia
Abban az esetben, ha a nyilvánossá tett szexuális tartalmú felvételeken 18. életévét be nem töltött személy szerepel, gyermekpornográfia közzétételéről van szó, ez akár nyolc év szabadságvesztést is jelenthet.

A polgári jog értelmében az áldozat személyiségi jogának megsértése miatt – többek között – sérelemdíjat követelhet.

Az üzleti ötlettől a börtönig – nemzetközi kitekintés
A bosszúpornóban világszerte többen is meglátták az anyagi haszonszerzés lehetőségét. Az erre szakosodott oldalak begyűjtötték a hasonló tartalmakat a bosszúszomjas jelentkezőktől, majd súlyos összegeket kértek az áldozatoktól a megszégyenítő tartalmak eltávolításért.
Nagy-Britannia az első ország, ahol már büntetőjogi kategóriává tették a bosszúpornót. Az Egyesült Államokban pedig több ítélet is született hasonló portálok üzemeltetőivel szemben: az elkövetőknek a 4-5 éves börtönbüntetés mellett komoly kártérítéssel is szembe kell nézniük, többek között zsarolás és személyes adatokkal való visszaélés miatt.

Mi számít hozzájárulás nélkül hozzáférhetővé tett tartalomnak?
Ha egy felhasználó személyes adatait az engedélye nélkül tették közzé az interneten vagy olyan képet, videót töltöttek fel róla, amit nem kíván a nyilvánossággal megosztani, nem adott engedélyt a közzétételére.
Olyan esetekben beszélünk hozzájárulás nélkül hozzáférhetővé tett tartalomról, amikor az adott személy hozzájárulása, engedélye nélkül tettek közzé az interneten vele vagy gyermekével kapcsolatos fénykép-, video- vagy hangfelvételt, illetve egyéb személyes adatot.

A megsértett jogi normák
Ptk. 2:45. § A becsülethez és jóhírnévhez való jog
2:45. § (1) A becsület megsértését jelenti különösen a más személy társadalmi megítélésének hátrányos befolyásolására alkalmas, kifejezésmódjában indokolatlanul bántó véleménynyilvánítás.
(2) A jóhírnév megsértését jelenti különösen, ha valaki más személyre vonatkozó és e személyt sértő, valótlan tényt állít vagy híresztel, vagy valós tényt hamis színben tüntet fel.
Ptk. 2:48. § A képmáshoz és a hangfelvételhez való jog
2:48. § (1) Képmás vagy hangfelvétel elkészítéséhez és felhasználásához az érintett személy hozzájárulása szükséges.
(2) Nincs szükség az érintett hozzájárulására a felvétel elkészítéséhez és az elkészített felvétel felhasználásához tömegfelvétel és nyilvános közéleti szereplésről készült felvétel esetén.
Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 5. §
5. § (1) Személyes adat akkor kezelhető, ha
a) ahhoz az érintett hozzájárul, vagy
b) azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés).
Btk. 219. § Személyes adattal visszaélés
219. § (1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva
a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy
b) az adatok biztonságát szolgáló intézkedést elmulasztja,
vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
(2) Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.
(3) A büntetés két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges adatra követik el.
(4) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.
Btk. 226. § Rágalmazás
226. § (1) Aki valakiről más előtt a becsület csorbítására alkalmas tényt állít, híresztel, vagy ilyen tényre közvetlenül utaló kifejezést használ, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés két évig terjedő szabadságvesztés, ha a rágalmazást
a) aljas indokból vagy célból,
b) nagy nyilvánosság előtt, vagy
c) jelentős érdeksérelmet okozva
követik el.
Btk. 226/A. § Becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése
226/A. § (1) Aki abból a célból, hogy más vagy mások becsületét csorbítsa, hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt készít, ha más bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

Btk. 226/B. § Becsület csorbítására alkalmas hamis hang- vagy képfelvétel nyilvánosságra hozatala
226/B. § (1) Aki abból a célból, hogy más vagy mások becsületét csorbítsa, hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt hozzáférhetővé tesz, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a bűncselekményt
a) nagy nyilvánosság előtt, vagy
b) jelentős érdeksérelmet okozva
követik el.
Btk. 227. § Becsületsértés
227. § (1) Aki a 226. §-ban meghatározottakon kívül mással szemben
a) a sértett munkakörének ellátásával, közmegbízatásának teljesítésével vagy közérdekű tevékenységével összefüggésben vagy
b) nagy nyilvánosság előtt
a becsület csorbítására alkalmas kifejezést használ, vagy egyéb ilyen cselekményt követ el, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
(2) Az (1) bekezdés szerint büntetendő, aki a becsületsértést tettlegesen követi el.
Btk. 228. § Kegyeletsértés
228. § Aki halottat vagy emlékét a 226. vagy a 227. §-ban meghatározott módon meggyalázza, vétség miatt az ott meghatározott büntetéssel büntetendő.

7.6. Tananyagegység

7.6.1.	Megnevezése	A Facebook tudatos használata

Mindig azt halljuk, hogy megosztani jó. A technológiának köszönhetően pedig meg tudjuk osztani ötleteinket, véleményünket, képeinket és videóinkat barátainkkal és másokkal. Megosztani az esetek többségében *valóban* jó. De ha nem gondoljuk át eléggé, hogyan osztunk meg dolgokat, akkor saját magunknak vagy másnak okozhatunk bajt vele. Ne felejtsd el azt sem, hogy amit az ismerőseiddel megosztasz, azt ők végső soron tovább oszthatják. Ezért fontos, hogy gondolkodj, mielőtt bármit megosztasz.

A SAJÁT DOLGAID
Amikor megosztasz magadról egy képet, videót, vagy olyan személyes dolgokat, mint például a telefonszámod, ne felejtsd el, hogy azok könnyen kerülhetnek olyan emberek elé, akiknek nem is akartad volna azokat elküldeni.
Ne ossz meg semmit olyankor, amikor nagyon eluralkodtak rajtad az érzelmek, akár a düh, a szomorúság vagy az izgalom. Előbb nyugodj le, és aztán döntsd el, hogy tényleg jó ötlet-e.
Következő lépésként tedd fel magadnak ezeket a kérdéseket:

- Azt szeretném, hogy az emberek ilyennek lássanak engem?
- Felhasználhatja ezt valaki arra, hogy bántson engem?
- Zavarna, ha ezt másokkal is megosztanák?
- Mi a legrosszabb dolog, ami történhet, ha ezt megosztom?

A jelszavak nem közösségiek:
Vannak olyan dolgok, amelyek megosztásával kapcsolatban igazán oda kell
figyelni. Néha előfordul, hogy a barátok, amíg még minden rendben van, megadják egymásnak a jelszavukat, de sajnos ez később aztán rémálommá válhat.

A képek örökké tartanak:
Van, aki azt képzeli, hogy ha barátjával vagy barátnőjével megoszt egy meztelen vagy szexi képet, azzal kifejezi a szerelmét vagy a bizalmát. Ilyen helyzetben legyél nagyon óvatos, és gondold meg: egy kép tovább tarthat, mint egy kapcsolat.
Ne felejtsd el, hogy ha valaki arra kér, hogy olyasmit ossz meg, amivel nem vagy kibékülve, jogod van nemet mondani. Aki szeret vagy tisztel téged, úgysem fog rád nyomást gyakorolni vagy fenyegetni téged.

Másodpercek alatt eltűnik, de talán nem végleg:
Egyes alkalmazások és közösségi oldalak azt ígérik, hogy a képeket vagy videókat néhány másodpercnyi megjelenítés után automatikusan törlik. De ezt meg lehet kerülni, például aki megnézi, az képernyőfelvételt készíthet a képről, ezért továbbra is okosan kell dönteni arról, hogy mit oszt meg az ember.

MÁSOK DOLGAI

Amikor mások elküldik neked a dolgaikat, az esetek többségében nem bánják, ha te is megosztod ezeket másokkal. De ha nem vagy biztos ebben, kétszer is gondold meg, mielőtt így teszel. Sőt, még jobb, ha megkérdezed az illetőtől, aki küldte, hogy nem baj-e, ha megosztod. Ez a helyzet akkor is, ha olyan fényképet vagy videót osztasz meg, amelyen mások is szerepelnek: kérdezd meg, mielőtt megjelölöd őket rajta, közzéteszed, vagy továbbítod.

- Ha valaki megoszt veled valamit, amin más is szerepel, tedd fel magadnak a következő kérdéseket:
- Aki ezt nekem küldte, szeretné, ha megosztanám?
- Aki szerepel benne, megengedte neki?
- Nekem hogyan esne, ha valaki ilyesmit megosztana úgy, hogy én szerepelek benne?

Ha az illetőre nem vet jó fényt, amit kaptál, ha kínos neki, vagy ha bánthatja őt, amennyiben máshoz is eljut, ne add tovább. Lehet, hogy aki neked küldte, tréfának szánta, de ha valamit nem a megfelelő ember lát, akkor előfordulhat, hogy a helyzet már sokkal kevésbé vicces.
Nagyon sokan vannak – különösen fiúk –, akikre a barátaik nyomást gyakorolnak, hogy osszák meg barátnőjük vagy barátjuk meztelen képeit. Nehéz lehet az ilyen nyomásnak ellenállni, de arra kell gondolnod, hogy mekkora bajt okozhatsz saját magadnak és barátnődnek /barátodnak, ha beadod a derekad.

HOGYAN HOZHATOD HELYRE, HA VALAMI BALUL SÜLT EL?
Néha mindenki hoz helytelen döntéseket. Ez nem jelenti azt, hogy ne kellene mindent megtenned, hogy helyrehozd a dolgokat.
Ha valami olyat osztottál meg, amit nem kellett volna, az első dolog, hogy megkéred az embereket, akiknek elküldted, hogy ne adják tovább.
Ha valaki más tett közzé valamit, amit te küldtél el neki, első lépésként kérd meg, hogy vegye le. Ez többnyire eredményes. Ne feledd, hogy addig ne csinálj semmit, amíg dühös vagy. Adj magadnak időt, hogy lenyugodj, és ha tudsz, beszélj az illetővel az interneten kívül.
Ha nem hajlandó levenni, ne próbálj azzal visszavágni, hogy megosztasz olyan privát dolgokat, amit ő küldött neked, vagy hogy zaklatod, vagy a barátaidat ráveszed, lendüljenek ellene támadásba. Ez ugyanis szinte mindig csak rontja a helyzetet. Másrészt minél inkább próbálsz visszavágni, annál inkább úgy nézhet ki a dolog, hogy a helyzet legalább annyira a te hibád is, mint az övé.
Ha megjelöltek egy fényképen, és ez nem tetszik neked, ne felejtsd el, hogy a fényképmegosztó és közösségi oldalak nagy részén leveheted a nevedet bármelyik képről, amelyen megjelöltek. A Facebookon az adatvédelmi beállításoknál megadhatod azt is, hogy ellenőrizni tudd a bejegyzéseket, amelyekben megjelöltek, mielőtt azok kikerülnének az idővonaladra: facebook.com/privacy.
Ha a Facebookon vagy és kellemetlennek érzed, hogy valakivel szemben saját magad fellépj, vagy nem igazán tudod, hogy mit mondjál, a Facebook egy közösségi jelentési funkciójában találsz néhány olyan üzenet mintát, amelyeket felhasználhatsz, illetve ez a funkció lehetőséget nyújt, hogy szülő, tanár vagy megbízható ismerős segítségét kérd.
Súlyosabb dolgok – például részleges vagy teljes meztelenséget ábrázoló kép vagy videó, rágalmazás (hazugság, amely a jó hírnevedet sérti), zaklatásodra vagy megfélemlítésedre használt tartalom – esetében kérheted az eltávolítását attól a helytől vagy szolgáltatástól, amelyen keresztül közzétették. Ilyen esetekben a rendőrségnek is bejelentést tehetsz. Ha olyan helyzetbe kerülsz, hogy valaki azzal fenyeget, hogy megoszt rólad egy meztelen képet, ha nem küldesz további meztelen képeket, vonj be egy megbízható felnőttet az ügybe, és azonnal fordulj a rendőrséghez. Ez elfogadhatatlan magatartás, számos országban törvénybe is ütközik.

7.7. Tananyagegység

7.7.1.	Megnevezése	Az Instagram tudatos használata

Képmás mint személyes adat. Az Instagram biztonságos használatához és a felelős megosztáshoz elengedhetetlenül szükséges a személyes adat fogalmának és a személyiségi jogok jelentőségének ismerete. A magyar adatvédelmi törvény alapján személyes adatnak minősül, és ezáltal védelemben részesül minden, azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személlyel kapcsolatba hozható adat, így különösen egy ember neve, azonosító jele, egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret, valamint az adatból levonható, az emberre (érintettre) vonatkozó következtetés. Így tehát egy fénykép vagy videó, amelyen az érintett képmása szerepel, személyes adatnak minősül. Az adatvédelmen túl a polgári jog a személyiségi jogok körében
védi az ember képmáshoz való jogát.
A személyes adatok védelme a felhasználó kezében van. Az Instagramon megosztott fényképeket és videókat alapértelmezés szerint bárki láthatja (hacsak nem közvetlenül osztják meg őket), de könnyen zártkörűvé

teheted a fiókodat, így csak az követhet, akinek ezt engedélyezed. Ehhez koppints a „Profile” (Adatlap) ikonra a jobb alsó sarokban, majd a profilképed mellett az „Edit Your Profile” (Adatlap szerkesztése) hivatkozásra. Legörgetve megnézheted, hogy be van-e kapcsolva a „Posts Are Private” (A bejegyzések zártkörűek) beállítás. Ha ki van kapcsolva, a kapcsoló átállításával zártkörűvé teheted a fényképeid elérését. (Az Android-felhasználóknak a „Profile” (Adatlap) ikonra és az „Edit Your Profile” (Adatlap szerkesztése) pontra kell koppintaniuk. Ügyelj rá, hogy engedélyezve legyen a „Posts are Private” (A bejegyzések zártkörűek) beállítás.) Az alkalmazás frissítése vagy újratelepítése esetén ellenőrizd, hogy a beállítások megfelelnek-e az általad kívántnak.

Az „Instagram Direct” automatikusan zártkörű. Ezzel a funkcióval bárki – még az is, akit nem követsz – úgy küldhet neked fényképet vagy videót, hogy azt rajtad kívül csupán legfeljebb 14 másik személy láthatja, és fűzhet hozzá bejegyzéseket. Ha követed az adott személyt, a kép a „Direct” (Közvetlen) mappádba érkezik. Ha nem követed az adott személyt, a kép a „Request” (Kérés) mappába érkezik, és a tőle származó „instagramok” egészen addig ide kerülnek, amíg jóvá nem hagyod az illetőt. Ha úgy döntesz, hogy figyelmen kívül hagyod az érintett személyt, akkor ő csak abban az esetben tud a későbbiekben instagramot küldeni neked, ha visszalépsz, és megváltoztatod ezt a beállítást.

A személyes adatok védelme soha nem tökéletes. Még ha a bejegyzéseid zártkörűek is, az adatlapod minden esetben nyilvános (bárki láthatja a profilképedet, a felhasználónevedet és a bemutatkozásodat). Összesen legfeljebb 10 sornyi szöveget adhatsz meg magadról, ezért a szülőknek és a gyermekeknek érdemes megbeszélniük, mi az, ami közölhető a bemutatkozó képernyőn.

Tartsd tiszteletben mások privátszféráját. Ha valaki más is szerepel az általad közzétenni kívánt fényképen, előbb győződj meg arról, hogy az érintett hozzájárul-e ahhoz, hogy az őt is ábrázoló képet megoszd, vagy, hogy őt (is) megjelöld rajta.

A bejegyzéseknek mindig van valamilyen hatása. Mielőtt megosztod, előbb gondold végig, hogyan érint az általad közölni kívánt tartalom másokat – függetlenül attól, hogy szerepelnek-e rajta vagy sem. Előfordulhat, hogy ismerősök például éppen azért sértődnek meg, mert nem szerepelnek a fényképen vagy a videón.

Gondold át a helyadatok megosztásának használatát. Az „Add to Photo Map” (Hozzáadás fotótérképhez) funkcióval helyszínt rendelhetsz hozzá a fényképhez. Alapértelmezés szerint ez a funkció ki van kapcsolva. Viszont ha egyszer már bekapcsoltad, az addig bekapcsolt állapotban marad, amíg ki nem kapcsolod. Később bármikor visszakapcsolhatod, de minden egyes megosztásnál érdemes végiggondolnod, valóban akarod-e, hogy mindenki tudja, hol készült a felvétel.

Megosztás az Instagramon kívül. Alapértelmezés szerint csak az Instagramon teszed közzé tartalmaidat, de az „E-mail”, „Facebook”, „Twitter” stb. beállításra, majd a „Share” (Megosztás) parancsra kattintva szélesebb körben is megoszthatod őket. Ha máshol is megosztasz, tartsd szem előtt az adott szolgáltatás adatvédelmi beállításait. A Twitteren például alapértelmezés szerint mindenki látja a megosztásaidat, ha nem állítod zártkörűre az adatlapodat. A Facebook alapértelmezés szerint csak az ismerőseiddel osztja meg az Instagramról közzétett tartalmakat. A Facebookon történő megosztást követően azonban megváltoztathatod ezt a beállítást úgy, hogy kiválasztod, és más közönséget jelölsz ki.

Megosztott tartalmaid sokat elárulnak rólad. Lehet, hogy magától értetődőnek tűnik, de ne felejtsd el, hogy a távoli jövőben is veled fogják azonosítani a korábban megosztott tartalmaidat, hiszen az interneten vagy okostelefonon közölt tartalmat gyakorlatilag lehetetlen eltüntetni. Ezért nem árt, ha átgondolod, milyen fényt vet rád később a ma közölt tartalom. Ha úgy gondolod, hogy hátrányosan befolyásolhat például egy állásra való jelentkezést, rosszat tehet egy kapcsolatnak, vagy felzaklathatja a rokonaidat, inkább ne oszd meg.

Kezeld a láthatóságodat! Azok a fényképek, amelyeken meg vagy jelölve (a videókon nem lehet megjelölni), az adatlapod „Photos of You” (Fényképek rólad) részében találhatók. (A „Photos of You” egyelőre csak az iPhone- és az Android-alkalmazásokban érhető el). Ezek mindenki számára láthatóak, hacsak nem teszed zártkörűvé a fiókodat. Mások is megjelölhetnek az általuk közzétett fényképeken, de ha az nem tetszik neked, elrejtheted a fényképedet az adatlapodról, vagy törölheted a bejelölést (ami ezután továbbra is látható marad az Instagramon, de nem kapcsolódik a felhasználónevedhez, és nem jelenik meg az adatlapodon). Ha nem szeretnéd, hogy a „Photos of You” (Fényképek rólad) részben automatikusan megjelenjenek a fényképek, ezt az „Add Automatically” (Automatikus hozzáadás) funkció kikapcsolásával tudod megakadályozni.

Koppints a „Profile” (Adatlap) ikonra, majd a „Photos of You” (Fényképek rólad) fülre, a fogaskerék gombra, és válaszd az „Add Manually” (Manuális hozzáadás) lehetőséget. (Az Android-felhasználóknak a „Photos of You” (Fényképek rólad) fülre, majd pedig a három kis négyzetre kell kattintaniuk.)

A teljes képet vizsgáld meg. A fénykép vagy videó háttere árulkodhat arról, hol és milyen körülmények között készült a felvétel, és mit csináltak akkor éppen a rajta szereplők. Biztosan szeretnéd közölni ezeket az információkat?

Médiatartalmaid bárhol megjelenhetnek. Az Instagram-videókat bármilyen webhelybe be lehet ágyazni, és nem szabad megfeledkezni arról, hogy mások bármilyen digitális tartalmat lemásolhatnak és megoszthatnak. Tehát még ha korlátozod is a közönséget, ne ossz meg olyasmit, aminek mások általi továbbadása bárki számára kellemetlenséget okozhat.

Használj erős jelszót, és ne áruld el másnak.Így bizonyos mértékig szabályozhatod, hogyan jelensz meg a közösségi médiában, mivel mások a jelszavad felhasználásával nem tudnak a nevedben fellépni. Használj eltérő jelszavakat a különböző szolgáltatásoknál. (A jelszóválasztással kapcsolatban a passwords.connectsafely.org oldalon találsz tanácsokat.)

A megjelöléseket törölheted. Csak az adott tartalom közzétevője tud megjelölni másokat a bejegyzésében, de – ha az adott személy adatlapja nyilvános – a közzétevő által megjelölt bármely személy törölni tudja a rá vonatkozó megjelölést. A megjelölést a bejegyzésben a felhasználónevedre koppintva tudod törölni, de csak akkor, ha a bejegyzés nyilvános, vagy ha követed a téged megjelölő személyt.

Szükség esetén letilthatsz másokat. Ha valaki zaklat, például ismételten személy jelöl meg neked nem tetsző fényképeken, sok közvetlen üzenetet küld, vagy félelmet keltő beszélgetésbe akar bevonni, letilthatod az illetőt, hogy ne tudjon megjelölni, közvetlenül keresni, ésa hozzászólásaiban megemlíteni téged. Letiltás esetén az adatlapodat sem láthatja és fiókodat sem találhatja meg. Felhasználó letiltásához lépj a letiltandó személy adatlapjára, válaszd a „Menu” (Menü) gombot a jobb felső sarokban, majd válaszd a B„Block User” (Felhasználó letiltása) lehetőséget. (Ha Androidot használsz, lépj a letiltani kívánt személy adatlapjára, és koppints a három kis négyzetre . Válaszd a „Block User” (Felhasználó letiltása) lehetőséget.)

Bejegyzéseidet is törölheted. Ha szeretnéd törölni a saját fényképeid vagy videóid valamelyikét, koppints a képernyőd jobb alsó sarka alatti három pontra (lásd a képernyőfelvételt), majd válaszd a „Delete” (Törlés) parancsot. Szintén ebből a menüből tudod megosztani és e-mailben elküldeni bejegyzésedet. De ha a Facebookon, a Twitteren vagy más szolgáltatásban is megosztottad a médiatartalmat, az Instagramról való törléssel azt máshonnan nem távolítja el.

Jól válaszd meg, kivel osztasz meg tartalmakat. Ahelyett, hogy az összes követőddel megosztanál egy fényképet, meghatározhatod, hogy ki láthatja azt. Koppints a jobb felső sarokban az „Instagram Direct” ikonra, és válaszd ki, kivel szeretnéd megosztani a fényképet (legfeljebb 15 személyt választhatsz).

Jelentsd a problémás bejegyzéseket. Jelentheted mások kifogásolható fényképeit, videóit vagy hozzászólásait – vagy az Instagram közösségi irányelveit megsértő felhasználókat. Koppints a bejegyzés alatt, a képernyő alján található pontokra, majd a „Report Inappropriate” (Kifogásolható tartalom jelentése) lehetőségre. Sürgős esetben a Súgóközpontból is küldhetsz e-mailt az Instagramnak. A Súgóközpont eléréséhez koppints a „Profile” (Adatlap) ikonra, majd a fogaskerék gombra . (Ha Androidot használsz, koppints a „Profile” (Adatlap) ikonra, majd pedig a három kis négyzetre .) Így eljutsz arra a képernyőre, ahol rákattinthatsz a „Support” (Támogatás) lehetőségre.

A „Request” (Kérés) listán található üzenetek figyelmen kívül hagyása. Amikor fényképeket vagy videókat küldenek neked, csak az általad követett személyek küldeményei kerülnek a „Direct” mappába. A másoktól érkező fényképek a „Requests” (Kérések) mappába érkeznek. Ha tehát nem szeretnél instagramot kapni olyan személytől, akit nem ismersz, hagyd figyelmen kívül a „Requests” (Kérések) mappában található képeket. Ha két hétig nem foglalkozol velük, a tartalom egyszerűen törlődik. Ha csak az általad ismert személyek képeit szeretnéd látni, korlátozd, hogy kiket követsz.

7.8. Tananyagegység

7.8.1.	Megnevezése	Youtube tudatos használata

https://www.youtube.com/yt/about/policies/#community-guidelines

7.9. Tananyagegység

7.9.1.	Megnevezése	LinkedIn tudatos használata

A Linkedin 2003-ban jelent meg és jelenleg a negyedik legnépszerűbb közösségi média csatorna az Egyesült Államokban. Középpontjában elsősorban a karrier áll, vagyis segíti a felhasználókat kapcsolatokat kiépíteni, és tartalmakat megosztani többek között a szakmabeliekkel, beleértve a kollégákat, a lehetséges munkavállalókat, üzleti partnereket, stb. A cégek számára pedig egyre jobb lehetőséget kínál a marketingre.

MIRE FIGYELJ, MIUTÁN LÉTREHOZTAD A LINKEDIN-FIÓKOD?

ÁLLÍTSD BE A NYILVÁNOS PROFILOD URL-JÉT!
Ahhoz, hogy a személyes profilod valóban professzionálisnak hasson – és persze, hogy könnyebb legyen megosztani mondjuk az önéletrajzodban -, érdemes személyre szabni a nyilvános URL-t.

ADJ A PROFILODHOZ HÁTTÉRKÉPET!
Miután a közösségi média csatornákon elterjed a háttérképek használata, a Linkedin sem hagyhatta ki, így 2014 júniusától elérhető a funkció. Ennek annyi előnye van a számodra, hogy egy kicsit személyesebbé teheted a profilod, ha saját fotót használsz. A Linkedin 1584 x 396 pixel felbontású képet javasol ide, ami lehet JPG, PNG vagy akár GIF fájl is, a lényeg, hogy 8 Mb alatt maradjon a mérete.

HASZNÁLD KI, HOGY HOGY LINKEKET HELYEZHETSZ EL A PROFILODBAN!
Ahelyett, hogy csak az alapértelmezett linkeket használnád a weboldalak felsorolásánál a Contact Info részben, hozzáadhatsz bármilyen URL-t, köztük olyat, amely a személyes portfoliódat tartalmazza, vagy más közösségi oldalakra mutatót. Ráadásul az egyes munkahelyek leírását is kibővítheted linkekkel. És azt se felejtsd el, hogy az egyes munkahelyekhez feltölthetsz prezentációkat, videókat vagy audiofájlokat is! Ami remek lehetőség arra, hogy érdekesebbé tedd az önéletrajzod.

SEO-ZD A LINKEDIN PROFILODAT!
Nem csak weboldalakat vagy blogokat lehet keresőoptimalizálni, hanem a linkedines profilodat is. Ezáltal többen fognak rád találni, ha azokat a kulcsszavakat használják, amelyeket Te is fontosnak tartasz. Ezeket a kulcsszavakat a profilod több részénél is megjelentetheted: a címsorban, az összefoglalóban, vagy a munkatapasztalataidnál.

RENDEZZ ÁT RÉSZEKET!
Amikor szerkesztés módban használod a profilod, akkor bizonyos szekcióknál átrendezheted az ott megjelenő információk sorrendjét. Ehhez csak a szerkesztés kiválasztása után az egyes elemek mellett megjelenő vonala fölé kell vinned az egeret, és ha megjelenik egy nyíl, akkor kattintással meg is ragadhatod az adott elemet.

MENTS EL KERESÉSEKET!
A Linkedin lehetővé teszi azt, hogy elments munkakereséseket. Ehhez csak a keresés után a jobb felső részen megjelenő Create search alertre-re kell kattintani, ahol beállíthatod, hogy napi vagy heti értesítést kérsz róla. Később törölheted azokat a kereséseket, melyek már nem fontosak a számodra, ha a “Manage” gombra kattintasz.

INDÍTSD EL A MUNKAKERESÉST!
Ezt a Job menüpontban éred el, de ha erre a linkre kattintasz, akkor szintén elindíthatod az aktív munkakeresés folyamatát. Ehhez csak ki kell töltened a megfelelő mezőket, majd bekapcsolni a funkciót.

FINOMHANGOLD A “JÓVÁHAGYÁSOKAT”!
Így talán nem ismerős, de ha úgy mondjuk endorsements, akkor nyilván mindenkinek beugrik, hogy mi is ez a funkció. Ez szépen működik, csak figyelned kell arra, hogy a megfelelő készségek, tudás legyen felsorolva, valamint, hogy a beállításoknál mi az, ami be van kapcsolva, és mi az, ami nem. A lehetőségeket ott találod az Endorsement részen: az “Add a new skill”-el vehetsz fel ide új elemeket, míg a box bal alsó sarkában lévő “Adjust endorsement settings”-re kattintva állathatod be, hogy hogyan működjön a jóváhagyások rendszere a Te esetedben. Természetesen törölhetsz is elemeket a szerkesztés ikonra (jobb felső sarok a boxban) kattintva.

LÉGY BEAZONOSÍTHATÓ!
Tedd lehetővé másoknak, hogy lássák, ki vagy, amikor megnézik a profiodat! Lépj be a beállításokba (a felső menüsorban a profilfotódra kattintva megjelenő legördülő menüben válaszd a Settings & Privacy lehetőséget), majd a Privacy résznél a “Profile viewing options” pontnál állíthatod be, hogy mit láthatnak belőled mások. Az alapértelmezett beállítás tanácsos, ha valóban a karriered előmozdítására használnád a Linkedint, a többi opcióval viszont jól lehet rejtőzködni.

HOGYAN ALAKÍTSD KI AZ “ÖSSZEGZÉST” A PROFILODNÁL?
A Linkedin profilod egyik legfontosabb része az összegzés, mely egyből a neved és a fotód alatt található összefoglaló leírás rólad. Ez az, ami meggyőzi arról az érdeklődőket, hogy tovább görgessenek lefelé. Itt kell magad eladni a munkáltatóknak vagy az ügyfeleknek, felkelteni a figyelmet. Ugyanúgy működik a dolog, mint egy weboldalnál: ez a hajtás feletti rész, ahol a leglényegesebb elemeknek meg kell jelenniük, különben visszalép a látogató. De mi kerüljön bele?

AZ ÖSSZEGZÉS NEM RÓLAD SZÓL
Talán meglepő lehet elsőre, de az összegzésednek nem rólad kellene szólnia. Ahogy egy weboldalnál is a rólunk oldal alapvetően nem rólunk, hanem az értékesítésről szól, úgy itt is az a lényeg, hogy "miként tudod kelendőbbé tenni a portékát". Nem az önéletrajzod kerül tehát ide, hanem a válaszok azon kérdésekre, hogy miként tudod megoldani az ügyfél problémáját? Milyen gondjaira kínálsz megoldást? Miért lesz jobb a munkáltató vagy ügyfél élete, ha téged bíz meg a munkával? Az olvasók ugyanis nem rajtad gondolkodnak, hanem magukon, hogy mennyiben tudod könnyebbé tenni az életüket. Ezért kell teljes mértékben az ő szükségleteikre és igényeikre összpontosítanod. És lehetőleg röviden kell választ adnod ezekre a kérdésekre, mert a látogatók nem feltétlenül fogják lenyitni az összefoglalást. Így mindössze egy-két mondatnyi helyed van a meggyőzésre. Utána jöhet a többi, de a meggyőzésre irányuló mondatoknak rövidnek kell lenniük, és előre kell kerülniük.

AZONOSÍTSD BE A KÖZÖNSÉGED!
Ki fogja elolvasni ezt az összegzést? Kit akarsz elérni vele? Milyen munkát keresel? És milyen személyekkel akarsz kapcsolatba lépni? Megint egy csomó kérdés, amelyekre meg kell fogalmaznod a választ ahhoz, hogy tudd, mit is kellene leírnod. A Linkedinen ugyanis a legkülönfélébb emberek jelen vannak, akik eltérő dolgokat keresnek ott. Egy HR-est például az érdekelhet elsősorban, hogy milyen tapasztalatot szereztél egy nagynevű cégnél. Ugyanakkor egy kis, startup talán olyan embert keres, akik képes neki abban segíteni, hogy nulláról felépítsen egy céget. Minél inkább sikerül leszűkíteni a célközönséged igényeire az összefoglalód, annál hatékonyabbá válik számukra.

INDULJ KI EGY LISTÁBÓL!
Vannak olyan elemek, amelyeket szeretnél, ha szerepelnének az összegzésedben? Ezeket még annak megírása előtt gyűjtsd össze, mert nagyban megkönnyítik majd a munkát. Mi lehet az a pár dolog, amit feltétlenül meg kell említened? A legfontosabb szakmai teljesítmények Mi az, ami megkülönböztet a többektől Egy idézet egy korábbi munkáltatótól Valami hiteles dolog a személyiségeddel kapcsolatban A keresett pozícióhoz kapcsolódó kulcsszavak Ezekről 3-4 rövid bekezdést fogalmazz meg úgy, hogy megkülönböztethetővé válj a többiektől. Ez lesz az, ami rád irányítja majd a figyelmet.

MARADJ TÖMÖR!
Ne felejtsd el, hogy ez egy összegzés, tehát nem ide kell kerülnie minden adatnak a legnagyobb részletességgel. Erre ott van a tapasztalatokról és a tanulmányokról szóló rész. Az összegzés lényege a figyelem felkeltése annak érdekében, hogy aztán továbbgörgessenek a profilodban.

FIGYELJ A KULCSSZAVAKRA!
A Linkedin összegzés második legfontosabb célja a figyelem felkeltésén túl az, hogy könnyen megtalálható legyél. Ehhez – akárcsak a SEO-ban – kulcsszavakat kell használnod. Melyek azok a kulcsszavak, melyekre a potenciális érdeklődők, azaz munkáltatók és ügyfelek rákeresnek veled kapcsolatban? A kulcsszavak mindig a céljaidtól és a közönségedtől függenek. Csak gondold át, hogy milyen keresésekre szeretnél a találati listán szerepelni, majd ezeket a kulcsszavakat helyezd el a leírásodban. Túlzásba persze nem kell esni, hiszen a többi részben is szerepeltethetsz majd kulcsszavakat.

HOGYAN ERŐSÍTSD A HITELESSÉGED A LINKEDINEN?
Mivel az emberek rendkívül szkeptikusak mindennel kapcsolatban, amit a weben találnak – sok a rossz tapasztalat -, ezért a Linkedin-profilodnál is oda kell figyelni arra, hogy maximálisan hitelesnek tűnjön. Hiszen, ha az emberek, akik rátalálnak a profilodra, megbízhatónak találnak, akkor nyilván nagyobb eséllyel akarnak veled dolgozni.

1. EMLÍTSD MEG MINDEN EREDMÉNYEDET! A leggyorsabb módja annak, hogy erősítsd a hitelességedet, ha minden eredményedről részletesen beszámolsz. Ez azt jelenti, hogy minden tapasztalatod felsorolod: az ügyfeleiddel, munkáltatóiddal kapcsolatos információkat, valamennyi munkatapasztalatodat, tanfolyamokat és az ezeken elért végzettségeket. Ha szerepelsz valamilyen listán, közreműködtél valamilyen projektben, akkor jelezd és linkeld! Ha felkerültél valamilyen releváns listára, ha valahol megemlítettek, ha írtál egy könyvet, közzétettél cikkeket, akkor azt tedd láthatóvá mindenki számára. Írd le azokat az eredményeket is, amelyeket az egyes munkáid során elértél! Még akár a címlapi képre is ráhelyezheted a megjelenéseidet, ha látványosan meg tudod tenni. Valahogy így: Ez alapján hitelesnek tűnik ez a profil? Elsőre legalábbis meggyőző.

2. SZEREZZ AJÁNLÁSOKAT! Ha bemutattad a teljesítményedet, az sokat segít, de ami még hatékonyabb, ha ajánlásokat szerzel azoktól, akikkel együtt dolgoztál vagy dolgozol. Az emberek ugyanis sokkal inkább megbíznak mások véleményében, mint a Tiédben, amikor magadról beszélsz. Annál is inkább, mert a Linkedinen annak a személynek a profilját is le tudják ellenőrizni, aki az ajánlást adta Neked. A cél tehát az, hogy minél több ajánlást összegyűjts. Ehhez annyit kell tenned, hogy felveszed a kapcsolatot azokkal, akikkel korábban együtt dolgoztál, és megkéred őket erre a szívességre. Nyilván olyanokat kérsz csak meg, akik jelen vannak a

Linkedinen. A legjobb persze, ha ezek az ajánlások olyanok, mint egy esettanulmány, tehát kiderül belőlük számszerűsítve, hogy mit tettél hozzá a cég eredményeihez. A statisztikák nem csak hitelesebbé teszik az ajánlást, hanem megmutatják azt, hogy mennyit érsz.

3. VIDEÓ AJÁNLÁSOK! Az ajánlások következő fokozatát a videós ajánlások jelentik. Minden munkahelyed szerkesztésénél a felület alján megtalálod az alábbi részt: A Linkedin itt lehetővé teszi, hogy videót is linkelj, ami azt jelenti, hogy az ügyfeleid akár egy YouTube videóban is elmondhatják Téged méltató mondataikat.

4. TÉGY KÖZZÉ HASZNOS TARTALMAKAT!
Végül pedig ne feledkezzünk meg arról, hogy a hitelességed kialakítása érdekében folyamatosan kommunikálnod kell. Mégpedig olyan tartalmakat kell közzétenned, melyek hasznosak és segítenek az embereknek, mivel ezáltal is növeld a bizalmukat irányodba. A legegyszerűbb, ha a Linkedin saját platformját használod a publikálásra. A bejegyzések linkjei megjelennek a Linkedin profilodban, így az emberek könnyen elérik őket, és kattintani tudnak rájuk. Természetesen a saját blogodban vagy akár mások blogjában megjelent bejegyzéseket is megoszthatod a Linkedinen, sőt akár közzéteheted csoportokban. Arról azonban győződj meg, hogy ezek valóban igényes tartalmak, mert ezek alakítják a Te személyes márkádat!

MIT POSZTOLJ A LINKEDINEN?
Mivel a Linkedin egy szakmai, kapcsolat-építő közösségi média csatorna, így a leginkább illeszkedő tartalmat az álláshirdetések és a karrier-információk alkotják. Egy céges oldal megfelelő eszköz arra, hogy a pontenciális alkalmazottak többet megtudjanak a cégről. Nézd meg például, hogy a Google, hogy használja a Linkedint. Megosztja a cégkultúrával kapcsolatos információkat, közzéteszi a munkavállalói tapasztalatokat, az alkalmazottak eredményeit, valamint tájékoztatást ad arról, hogy milyen területen keresnek szakembereket.

CÉGES HÍREK
Amellett, hogy közzéteszed a munkalehetőségeket és a karrier-információkat, céges híreket is megoszthatsz a Linkedinen. Ahogy például a Facebook csinálja. Ahhoz, hogy meg tudd állapítani, mely posztok érik el a legnagyobb elköteleződést – a legjobb bejegyzések azok, melyek a legtöbb megtekintéssel, kattintással vagy elköteleződési aránnyal bírnak -, használd a céges oldalad analitikáját. Ennek segítségével tudod megállapítani, hogy mi az, amire reagál a közönséged. (Ehhez itt nyújt segítséget a Linkedin.) Ezután már csak az a dolgod, hogy hasonló bejegyzéseket készíts, vagy pedig a sikeres bejegyzéseid néhány hét elteltével ismét közzétedd. Ha nagyobb elköteleződést szeretnél elérni, akkor érdemes a Linkedinen is bevetni a képeket és a videókat. A Linkedin szerint a képek általában 98 százalékkal nagyobb hozzászólási arányt érnek el, míg a közvetlenül lejátszott Youtube videóknak 75 százalékkal magasabb a megosztási aránya.

SZAKMAI TARTALOM
Néha persze nincs elég olyan tartalmad, mely az előbb említett témákról – karrierről, állásról, céges eredményekről – szól. Ilyenkor közzétehetsz olyan tartalmakat is, melyek a célközönségedbe tartozó szakemberek számára érdekes lehet, például tanulmányokat vagy képzésekről szóló tájékoztatást, ahogy például a Hubspot is. Ehhez persze nem árt tudni, hogy ki is a célközönséged, azaz kik követnek téged a Linkedinen. A róluk szóló analitikát így éred el. Kiderül például, hogy milyen iparágakból jönnek, akik érdeklődnek a céged iránt, ami már jó támpontot jelent a posztok témájának meghatározásához.

MIRE FIGYELJ KÉSŐBB, A LINKEDIN HASZNÁLATA SORÁN?
Régebb óta van Linkedin profilod? Mikor nézted át utoljára az ott megadott információkat? Akkor talán fuss neki, és a most felsorolt dolgokat feltétlenül tekintsd át!

FRISSÍTSD A KÉPEKET ÉS A LEÍRÁST!
Ha történt valami változás veled (vagy a cégeddel) mondjuk az elmúlt 12 hónap során, amiről úgy érzed, hogy érdemes megmutatni az embereknek, akkor frissítsd a megjelenő képeket a profilodnál. Ha egy cégről van szó, akkor ez lehet például egy új termék vagy szolgáltatás bevezetése, esetleg egy újramárkázás, új imidzs kialakítása, új design a weboldaladon. Arra is figyelj, hogy a korábban közzétett leírás megfelel-e a jelenlegi állapotodnak, azt tükrözi, amit teszel, pontosan megmutatja-e, hogy ki is vagy jelen pillantban. Ha megjelent egy új videó rólad vagy a cégedről, akkor azzal is bővítsd ki a Linkedin profilodat. Végül, ellenőrizd, hogy a Linkedin profilod megjelenése azonos a céged más online megjelenéseivel!

ELLENŐRIZD A TAPASZTALATOK RÉSZT!
Gyakori hiba, hogy nem egészen friss az Experience rész a Linkedin-profiloknál. Pedig ez rontja a hitelességed és a szakmaiságod. Győződj meg arról, hogy a jelenlegi munkahelyedet helyesen adtad meg! Ha szükséges, akkor rendezd újra a sorrendet! Egyszerűen csak fogj meg egy részt, és vidd a megfelelő pozícióba úgy, hogy a legrelevánsabb tapasztalatok legyenek legfelül!

ELLENŐRIZD A WEBOLDAL-LINKEKET! Mivel a weboldalak linkjei gyakran változnak, így ugyanilyen gyakran kellene ellenőrizned, hogy a Linkedin profildnál megadott linkek helyesek-e. Ehhez a névjegyednél a Contact Infóra kell kattintani, ahol legördülnek a lehetőségek, többek között a linkek szerkesztése. Nem muszáj a legördülő lehetőségek közül választani. Ha az Other opciót választod, akkor meghatározhatod, hogy mi legyen a linked horgonyszövege.

RENDEZD EL A KAPCSOLATAIDAT! Ha a felső menüsorban a My Network címkére kattintasz, akkor a legördülő menüben kiválaszthatod a Connection linket. Erre rákattintva felsorolja a kapcsolataidat, melyek közül érdemes kidobálni azokat, melyek nem relevánsak. Ugyanakkor azok számára innen küldhetsz üzenetet is, akikkel szorosabbra fűznéd a viszonyodat. Érdemes.

TEKINTSD ÁT AZ AKTIVITÁSODAT! A frissítések rendszeres megosztása az egyik legjobb lehetőség arra, hogy növeld a láthatóságodat és a Linkedin profilod látogatószámát. Ha névjegyednél a “View profile as” melletti nyíl fölé viszed az egeret, akkor a megjelenő menüből kiválaszthatod a View recent activity linket, mely megmutatja, hogy melyik frissítésed miként teljesített. A Linkedinen optimális lenne a legalább három naponkénti frissítés, illetve olyan tartalmak megosztása, melyek nem csak relevánsak rád vagy a márkádra tekintve, de a célközönségedet is érdekelhetik.

HOGYAN ÉRHETSZ EL TÖBB MEGTEKINTÉST ÉS MEGOSZTÁST A LINKEDINEN?

1. ÍRJ CSAK SZÖVEGES POSZTOKAT!
Közösségi média tippeknél biztos találkoztál már azzal a tanáccsal, hogy az emberek általában nagyobb eséllyel osztanak meg képet vagy videót. Habár ez igaz lehet mondjuk a Facebook esetében, a Social Media Examiner szerint nem működik a Linkedinen. Ahogy az még kevésbé, amikor linkeket osztasz meg, amihez általában behúz egy képet is a rendszer. Ugyanakkor, ha kép és linkek nélküli, pusztán szöveges posztot osztasz meg, akkor az jelentősen több reakciót válthat ki. Egy Linkedin poszt hossza most már elérheti az 1300 karaktert is. Ez persze nem túl hosszú, néhány bekezdéses bejegyzést jelent. Ha olyan a témád, hogy nagyobb teret kíván, akkor rendkívül egyszerűen publikálhatsz is cikket a Linkedin beépített blog-platformján. Mivel a Linkedin csak a szöveges posztod elejét mutatja meg a hírfolyamban, ezért azt a történetmesélési technikát kell alkalmaznod, miszerint a legfontosabb, a felhasználót megragadó mondatok az elejére kerüljenek. Ha szeretnél reakciókat a posztodra, akkor itt is érdemes kérdeseket feltenned, álláspontot megfogalmaznod. Ha pedig képet és linket is tennél a bejegyzésedhez, akkor azt ne a posztba, hanem a kommenteknél helyezd el!

2. LÁJKOLD A SAJÁT POSZTJAIDAT!
Miért jelenik meg egy Like gomb a saját posztod mellett? Vajon a Linkedinen nem néz ki furcsán, ha a saját bejegyzésedet lájkolod? Ott egy gomb, amiről tudod, hogy nem kellene megnyomnod. De miért is? Hiszen, ha lájkolod a posztod, akkor javítod az elkötelezettséget. Ugyanez vonatkozik a saját kommentjeidre is. Ez különösen akkor hasznos, ha mások is hozzászóltak a bejegyzéshez, mert így jelzést kapnak a hozzászólásra érkezett lájkról, és ez lehet, hogy őket is további közreműködésre ösztönzi. És, hogy miért is hasznos a saját posztjaidat vagy kommentjeidet lájkolni? Azért, mert az emberek sokkal sokkal könnyebben lépnek interakcióba akkor, ha már más megtette az első lépést. Ez olyan, mint a táncparkettre lépni: sokkal nehezebb elsőként rálépni, mint akkor, ha már sokan táncolnak ott előtted.

3. HASZNÁLD KI A HOZZÁSZÓLÁS LEHETŐSÉGÉT!
Mindig figyelj azokra, akik időt szakítottak arra, hogy egy kommentet hagyjanak a posztod alatt! Ha lájkolod a posztjaikat vagy válaszolsz rájuk, akkor megnöveled az esélyét annak, hogy tovább folytatódik a társalgás. Azok az emberek, akik hozzászóltak, ilyenkor jelzést kapnak arról, hogy válasz érkezett a hozzászólásukra, aminek eredményeként további elkötelezettséget érhetsz el, ideális esetben pedig akár a bejegyzésedet is megosztják.

4. KÉSZÍTS ÉS OSSZ MEG NATÍV VIDEÓKAT!
A Linkedin mobil appjával videókat tudsz készíteni, vagy akár előre elkészített videót is fel tudsz tölteni. Keresd a videókamera ikont az app legfrissebb verziójában, a jobb felső sarokban! Csakúgy mint a Facebookon, a Linkedinen is automatikusan, de némán indulnak el a videók a hírfolyamban. Ugyanakkor szöveget nem tudsz rá írni, így magának a videónak kellene tartalmaznia a szöveget. Ehhez valamilyen videószerkesztő programra lesz szükséged. Mivel a videó még újdonság a Linkedinen, ezért a használatával ki tudsz tűnni a többiek közül. Érdemes tehát kipróbálni, és figyelni, hogy milyen eredményeket érsz el vele.

5. TEDD NYILVÁNOSSÁ A FRISSÍTÉSEIDET!
2017 júliusa óta lehetőség van arra, hogy nyilvánossá tedd az állapotfrissítéseidet. Ehhez ellenőrizd a beállításaidat és válaszd azt a lehetőséget, miszerint bármely posztod nyilvános lehet. Ezt az asztali felületen teheted meg, ha először rákattintasz a Me, majd a Setting & Privacyre. Válaszd ki a Privacy fület, ahol megtalálod a Blocking and hiding részt. Itt kiválasztod a Followers részt, ahol beállítod, hogy mindenki láthassa az

állapotfrissítéseidet. Ez azonban még nem lesz elég. A bal oldali menüben látod a Profile Privacy pontot, amire kattintva válaszd ki a megjelenő opciók közül az Edit your public profile-t. Az itt megjelenő oldal jobb oldalán találod a Customize Your Public Profile részt, ahol beállíthatod, hogy mi és ki számára legyen nyilvános. A Posts & Activities mellett is legyen pipa. Ezek után már bármely posztodat nyilvánossá teheted, ehhez a mező alatti részen kell a Public lehetőséget választanod a legördülő menüből. A Linkedin leírását itt találod minderről.
