KOMISIONERI PËR TË DREJTËN
E INFORMIMIT DHE MBROJTJEN
E TË DHËNAVE PERSONALE

KUADRI
I AFTËSIMIT TË MËSUESVE TË SHKOLLAVE 9-VJEÇARE
MBI MBROJTJEN E TË DHËNAVE PERSONALE TË NXËNËSVE

shoqëruar me një shpjegues të detajuar
për çdo aftësim si dhe këshilla për prindërit

www.idp.al

KONFERENCA NDËRKOMBËTARE E KOMISIONERËVE
TË TË DHËNAVE DHE PRIVATËSISË

GRUPI NDËRKOMBËTAR I PUNËS PËR EDUKIMIN DIGJITAL

KOMISIONERI PËR TË DREJTËN E INFORMIMIT
DHE MBROJTJEN E TË DHËNAVE PERSONALE

Prezantojnë

KUADRIN E AFTËSIMIT TË MËSUESVE TË SHKOLLAVE 9-VJEÇARE MBI MBROJTJEN E TË DHËNAVE PERSONALE TË NXËNËSVE

KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE

Përmbledhje

KONFERENCA E 38-TË NDËRKOMBËTARE E KOMISIONERËVE TË MBROJTJES SË TË DHËNAVE DHE PRIVATËSISË

Marrakesh, 18 tetor 2016

Rezolutë për Miratimin e një Kuadri Ndërkombëtar Aftësimi mbi Edukimin për Privatësi

Konferenca e 38-të Ndërkombëtare e Komisionerëve të Mbrojtjes së të dhënave dhe Privatësisë:

Duke rikujtuar marrëveshjet ndërkombëtare, veçanërisht atyre që u referohen të drejtave të fëmijëve:

- Deklaratës së Gjenevës mbi të Drejtat e Fëmijës, 26 shtator 1924;
- Konventës së Kombeve të Bashkuara mbi të Drejtat e Fëmijës, 20 nëntor 1989;

Duke pasur parasysh rekomandimet ndërkombëtare në lidhje me edukimin e fëmijëve dhe adoleshentëve, konkretisht:

- Rekomandimin Rec(2006)12 të Komitetit të Ministrave të Këshillit të Evropës drejtuar shteteve anëtare, mbi fuqizimin e fëmijëve në ambientin e ri të informacionit dhe komunikimeve, 27 shtator 2016;
- Deklaratën e Komitetit të Ministrave të Këshillit të Evropës mbi mbrojtjen e dinjitetit, sigurisë dhe privatësisë së fëmijëve në internet, 20 shtator 2008;
- Rekomandimin e OECD-së drejtuar Këshillit mbi Mbrojtjen e Fëmijëve në Internet, 16 shkurt 2012;
- Rezolutën e UNESCO-s mbi problematikat që lidhen me internetin, përfshirë aksesin në informacion dhe dije, lirinë e shprehjes, privatësinë dhe dimensionet etike të shoqërisë së informacionit, miratuar në nëntor 2013, gjatë sesionit të 37-të;

Duke iu referuar Deklaratave Ndërkombëtare të krijuara për të mbështetur Shtetet, në përpjekjet e tyre afatmesme dhe afatgjata, për të nxitur edukim cilësor dhe për ta bërë edukimin prioritet për të gjithë, përfshirë edukimin për privatësi:

- Deklaratës së Incheon-it, të 2015-ës së UNESCO-s, e cila përcakton Edukimin 2030: Drejt edukimit cilësor gjithëpërfshirës dhe të drejtë dhe gjatë gjithë jetës për të gjithë Kuadri për Veprim, për të promovuar sidomos edukimin qytetar botëror duke u bazuar në Teknologjinë e Informacionit dhe Komunikimit (ICT);

Duke rikujtuar dy Rezolutat e Konferencës së 30-të Ndërkombëtare të Komisionerëve të Mbrojtjes së të Dhënave dhe Privatësisë në 2008-ën:

- Rezolutën mbi Mbrojtjen e Privatësisë në Shërbimet e Rrjeteve Sociale;

- Rezolutën mbi Privatësinë e Fëmijëve në Internet, e cila nxiste Komisionerët të zhvillonin programe të edukimit digjital, veçanërisht për të rinjtë;

Duke rikujtuar Rezolutën e Konferencës së 35-të Ndërkombëtare të Komisionerëve të Mbrojtjes së të Dhënave dhe Privatësisë së 2013-ës, mbi Edukimin Digjital për të Gjithë, e cila rekomandonte Komisionerët të:

- Promovojnë edukimin mbi mbrojtjen e të dhënave dhe privatësisë në programet e aftësimit digjital;
- Marrin pjesën në trajnimin e personave të ndërmjetëm, duke organizuar ose bashkëpunuar për "trajnimin e trajnerëve" të mbrojtjes së të dhënave dhe privatësisë;

Duke kuptuar se, për shumë Shtete, edukimi digjital i nxënësve, është sot një prioritet për veprim, në nivel kombëtar ose nën-kombëtar të qeverisjes;

Duke pranuar se sipas sistemeve të juridiksionit të anëtarëve, politikat në fushën e edukimit shkollor varen nga nivelet e ndryshme të qeverisjes dhe se ligjet që kanë të bëjnë me mbrojtjen e të dhënave, mund të ndryshojnë nga vendi në vend dhe se kjo rezolutë mundet gjithsesi të jetë kuptimplotë edhe në këto kushte;

Duke pasur parasysh se me qëllim që individët të bëhen në aktivë në mënyrë të efektshme në shoqërinë e sotme digjitale dhe në ekonominë digjitale, është e rëndësishme që të rritet ndërgjegjësimi i i fëmijëve që tani, sapo që ata nisin shkollën, në lidhje me pasojat e përdorimit dhe shkëmbimit të të dhënave, ashtu si edhe në lidhje me një bazë të përbashkët të aftësive konkrete dhe praktike në lidhje me mbrojtjen e të dhënave dhe privatësinë; dhe sa i takon kësaj, evidentimi i problematikave të mbrojtjes së të dhënave si pjesë e edukimit për aftësimin për privatësi, përshtatur me specifikat kombëtare, është një element thelbësor i edukimit qytetar dhe respektimit të së drejtave të njeriut;

Duke pohuar që, pavarësisht cilësisë së burimeve pedagogjike të prodhuara në lidhje me mbrojtjen e të dhënave, ka mungesë trajnimi për stafin arsimor në lidhje me mbrojtjen e të dhënave dhe privatësinë, me përjashtim të disa vendeve;

Duke rikujtuar që trajnimi i stafit arsimor ka ndikim në mësimdhënien e nxënësve dhe se shkollat duhet të kenë mjetet për të edukuar qytetarët mbi mënyrat e përdorimit të përgjegjshëm dhe etik të teknologjive;

Duke marrë në konsideratë që autoritetet e mbrojtjes së të dhënave, për shkak të ekspertizës së tyre, në bashkëpunim me stafin arsimor, përfaqësuesit e qeverisjeve dhe aktorë të tjerë të fushës, mund të japin kontribut të dobishëm në këtë trajnim;

Duke përcaktuar se, sa i takon kësaj, është e nevojshme të propozohet një bazë e përbashkët aftësish konkrete dhe praktike brenda një Kuadri Ndërkombëtar Aftësimi për mësimdhënien e nxënësve në lidhje me mbrojtjen e të dhënave dhe privatësinë, për stafin arsimor.

Autoritetet e pranishme në Konferencën e 38-të Ndërkombëtare të Komisionerëve të Mbrojtjes së të Dhënave dhe Privatësisë vlerësojnë si prioritet të rëndësishëm rekomandimin e veprimeve të mëposhtme:

- Të përfshihet edukimi mbi mbrojtjen e të dhënave dhe privatësinë në programet e studimit dhe në kurrikula;
- Të trajnohet stafi arsimor mbi mbrojtjen e të dhënave dhe privatësinë, duke u ofruar atyre si njohuri thelbësore ashtu edhe ekspertizë praktike në këtë sferë, duke u mundësuar atyre që të ndihmojnë të rinjtë të zhvillojnë mendimin kritik mbi mënyrën se si informacioni personal përdoret;
- Me këtë në mendje, të iniciohen aktivitete trajnuese, të cilat janë të fokusuara si në përfitimet ashtu edhe në risqet që vijnë nga përdorimi i teknologjive të reja dhe praktikat që na mundësojnë të jetojnë në një ambient digjital me siguri, qartësi dhe respekt të së drejtave individuale.

Rrjedhimisht, autoritetet e pranishme:

1. Miratojnë Kuadrin Ndërkombëtar të Aftësimit për nxënësit në lidhje me mbrojtjen e të dhënave dhe privatësinë bashkëlidhur si aneks dhe tërheqin vëmendjen e qeverive dhe sidomos të autoriteteve përgjegjëse për edukimin ashtu si edhe të aktorëve të tjerë që punojnë në fushën e edukimit sa i takon rëndësisë së:
   - Promovimit në bashkëpunim me autoritetet e mbrojtjes së të dhënave të përdorimit dhe zhvillimit praktik të Kuadrit të Aftësimit, si pjesë e programeve të studimit apo kurrikulës dhe të trajnimit të stafit arsimor, pavarësisht lëndës që ata japin;
   - Të inkurajimit të kërkimeve në pedagogjikë dhe didaktikë që kanë të bëjnë me mbrojtjen e të dhënave dhe privatësinë, në mënyrë që zhvillimi i aktiviteteve dhe burimeve në këtë fushë, të bazohet në studimet shkencore dhe eksperiencën profesionale.
2. Mandatojnë Grupin Ndërkombëtar të Punës mbi Edukimin Digjital për të:
   - Garantuar që autoritetet e mbrojtjes së të dhënave të mund të propozojnë apo kontribuojnë, në bashkëpunim me autoritetet kombëtare qeveritare dhe aktorët e fushës, prodhimin e burimeve pedagogjike të përshtatura me kuadrin e aftësive specifike të trajtuar dhe grup-moshën e përfshirë;
   - Garantuar ndjekjen e progresit të bërë në zhvillimin e aftësive të mbrojtjes së të dhënave dhe privatësisë në lidhje me edukimin digjital në programet edukative.

Komisioni Federal i Tregtisë së SHBA-ve abstenoi për shkak se rezoluta miraton një kuadër të unik ndërkombëtar, pa pranuar se ekzistojnë qasje të tjera që reflektojnë diversitetin e ligjeve të privatësisë dhe vlerave kulturore nëpër botë, të cilat mund të përmbushin gjithashtu synimin e përbashkët të promovimit të edukimit digjital.

Hyrje

Pse duhet një kuadër ndërkombëtar për trajnimin e mbrojtjes së të dhënave?

Në epokën digjitale, edukimi i përgjegjshëm, etik dhe i civilizuar në përdorimin e teknologjive të reja është një prioritet për veprim, veçanërisht për nxënësit në shkolla.
Një komponent kryesor i edukimit digjital është adresimi i mbrojtjes së të dhënave personale dhe privatësisë. Mësuesit kanë një rol kyç në këtë edukim digjital të qytetarëve.
Përvetësimi i njohurive kritike dhe kuptueshmëria e të drejtave digjitale dhe përgjegjësive, zhvillimi i aftësive të të menduarit kritik tek të rinjtë drejt përdorimit të të dhënave personale, rritja e ndërgjegjësimit për riskun dhe mësimdhënia e praktikave për të mundësuar që njerëzit të lundrojnë në mjedisin digjital me besueshmëri, kthjelltësi dhe respekt për të drejtat e çdokujt – këto janë objektivat që duhen arritur.
Në mënyrë që të ndihmohen mësuesit, autoritetet e mbrojtjes së të dhënave – me ekspertizën e tyre në këtë fushë – menduan se ishte e nevojshme për të projektuar një trajnim kuadër për nxënësit, dedikuar specifikisht mbrojtjes së të dhënave, për përdorim në programet zyrtare shkollore dhe në kurset e edukimit për mësuesit, pavarësisht nga disiplina e veçantë e mësuar.
Megjithëse mund të pësojë ndryshime duke adresuar qëllime edukuese specifike, qasje të ligjeve të mbrojtjes së të dhënave të rëndësishme për secilin shtet, kuadri është projektuar që të ketë një dimension ndërkombëtar.
Pse? Sepse ky është një problem madhor që prek të gjithë shtetet pa dallim; sepse synon të krijojë **një bazë të përbashkët konkrete dhe operacionale të aftësimit për mbrojtjen e të dhënave personale** që mund të përdoret nga të gjithë; dhe sepse qëllimi i saj është të trajtojë botën e edukimit si një të tërë.
Ja pse ky kuadër, projektuar me iniciativën e Grupit Ndërkombëtar të punës për Edukimin Digjital që koordinohet nga Autoriteti Francez i Mbrojtjes së të Dhënave Personale (CNIL), u miratua nga të gjithë autoritetet e mbrojtjes së të dhënave në Konferencën e 38-të Ndërkombëtare të Komisionerëve të Mbrojtjes së të Dhënave dhe Privatësisë në tetor 2016[1].

[1]Ky kuadër është projektuar nga autoriteti Francez i mbrojtjes së të dhënave (CNIL), me ndihmën e paçmueshme të autoriteteve të mbrojtjes së të dhënave, pjesë e Grupit Ndërkombëtar për Edukimin Digjital. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale është anëtar i grupit të punës ndërkombëtar që prej krijimit të tij në vitin 2013. Gjithashtu, janë marrë këshilla të rëndësishme të specialistëve të arsimit dhe ekspertëve me Shërbimet Edukative të Këshillit të Evropës.

Mbi Kuadrin

Qëllimi i këtij seti parimesh mësimi është për t'iu dhënë nxënësve njohuritë, kompetencat dhe aftësitë në bazën e përbashkët të kompetencave konkrete dhe operacionale të kuadrit të aftësimit të mbrojtjes së të dhënave.

Ky kuadër i prezantuar këtu ka nëntë **parime themelore;** njohja dhe kuptueshmëria e këtyre është një prioritet.

Një bllok me kompetenca të përgjithshme është identifikuar për çdo parim. Ato janë vendosur dhe lidhur në mënyrë që të arrijnë një balancë tematike progresive. Megjithatë, mësuesit do jenë të aftë për ti përdorur ato, edhe duke ndjekur progresionin e sugjeruar në dokument apo në një mënyrë të veçantë si pjesë e udhëzimit të tyre.

Secili nga parimet u analizua në kuadër të **njohurive dhe aftësive,** me përthithjen e njohurisë apo aftësisë që ndikon në aftësinë e studentit për të thënë *"unë e di" dhe/ose "unë mundem"*. Këto **përshkrues,** si edhe çfarë mbulojnë termat "njohuri" dhe "aftësi", janë përcaktuar në terminologjinë e propozuar bashkangjitur në këtë dokument.

Marrëveshja e arritur në një bazë të përbashkët të aftësive dhe njohurive konkrete është hapi i parë në përhapjen dhe promovimin e mbrojtjes së të dhënave personale dhe privatësisë në programet edukative.

Hapa dhe masa të tjera veprimi janë të rëndësishëm për të arritur me sukses përpjekjet për edukimin digjital, të cilat janë:

- Mënyra se si mësuesit zbatojnë këto parime mësimi në ambientet e klasave;
- Identifikimi, **bazuar në grup-moshën e konsideruar,** e shkallës së thellësisë së nevojshme për çdo element njohurie dhe aftësie; dhe
- Disponueshmëria e **burimeve edukuese dhe trajnuese** për mësuesit dhe studentët e tyre.

[1/9] Të dhënat personale

Qëllimi: kuptueshmëria e konceptit të të dhënave është thelbësore. Nocionet e pseudonimit dhe fshehja e identitetit të dikujt dhe metadata janë gjithashtu të shpjeguara. Studenti mëson gjithashtu se disa të dhëna personale mund të konsiderohen veçanërisht sensitive, për shkak të natyrës intime të jetës private dhe/ose të dhënat mund të jenë burim i diskriminimit të mundshëm ose ato mund t'i referohen të miturve. Si përfundim njohja me termat e mbledhjes së të dhënave dhe përpunimit ndihmon në kuptimin e konceptit të të dhënave personale.

Rezultatet e NJOHURIVE

- Unë kuptoj se çfarë përfshihet në konceptin e të **dhënave personale,** përcaktuar si çdo e dhënë – e bërë ose jo publike - për një individ të identifikueshëm;
- Unë e di dhe e kuptoj konceptin e **pseudonimit dhe fshehjen e identitetit të dikujt;**
- Unë e di se, varur nga mënyra se si përpunohen, të dhënat mund të lejojnë identifikimin e individëve;
- Unë e di se disa **të dhëna teknike** mund të bëjnë të mundur identifikimin e individëve; që dokumentet e skanuara dhe fotot kanë të ngulitur **metadata** që përshkruajnë përmbajtjet e tyre dhe se aktiviteti online mund të lërë **gjurmë** (cookies, historiku i kërkimit, etj) të cilat mund të përmbajnë të dhëna personale;
- Unë e di se ka të dhëna **të cilat mund të konsiderohen si vecanërisht sensitive, sipas shteteve,** dhe në të cilat, për shembull përmbajnë informacion lidhur me **minorenët, origjinat e njerëzve, besimet apo bindjet politike dhe fetare, profili biometrik dhe gjenetik, shëndeti dhe/ose jeta seksuale.**

Rezultatet e AFTËSIVE

- Unë mund të jap shembuj të të dhënave personale që mund të identifikojnë individë në mënyra direkte (gjendja civile, foto e një studenti në klasë, etj) dhe të dhënat teknike që mund të monitorojnë aktivitetet e një personi dhe ti identifikojë ato (cookies, të dhënat e gjeolokalizimit, etj.);
- Unë mund të jap shembuj të të dhënave sensitive (p.sh. të dhënat shëndetësore, profile gjenetike, jeta seksuale…).

E DHËNË PERSONALE ËSHTË ÇDO INFORMACION PËR NJË PERSON FIZIK I CILI ËSHTË I IDENTIFIKUAR OSE I IDENTIFIKUESHËM.

Duhet të kujdesemi që institucionet publike dhe private, kur përdorin të dhëna personale, t'i përmbahen ligjit.

CILAT JANË TË DHËNAT E TUA PERSONALE?
Shembuj të të dhënave personale:

Emri - Mbiemri
Adresa
Fotografia
Shenjat biometrike
Profesioni - Kualifikimet
Të ardhurat

Çdo e dhënë në lidhje me një person fizik e cila e bën të identifikueshëm drejtëpërdrejtë apo tërthorazi quhet e dhënë personale.

Të dhënat sensitive
Të dhënat sensitive janë një kategori e caktuar e të dhëna personale e cila përmban informacion më sensitiv për individin. Të dhëna sensitive janë të dhënat që tregojnë:

- origjinën racore ose etnike,
- mendimet politike,
- anëtarësimin në sindikata,
- besimin fetar apo filozofik,
- dënimin penal,
- të dhëna për shëndetin dhe jetën seksuale.

Për t'u thelluar më shumë:

https://youtu.be/tysTgs3FIaM

http://www.idp.al/wp-content/uploads/2016/11/Udh%C3%ABzuesi_per_te_dhenat_sensitive.pdf

[2/9] Privatësia, liritë civile dhe mbrojtja e të dhënave personale

Qëllimi: E drejta e mbrojtjes së të dhënave personale gjendet në të drejtat e njeriut, liritë civile, vlerat demokratike dhe qytetaria. Është gjithashtu një garanci e rëndësishme e respektimit të privatësisë.

Rezultatet e NJOHURIVE

- Unë e di se çfarë janë të drejtat e njeriut dhe liritë civile dhe mund ti citoj ato;
- Unë e di se këto parime dhe vlera demokratike ushtrohen po aq në botën reale si në atë virtuale;
- Unë e kuptoj konceptin e privatësisë, të drejtën e privatësisë dhe nevojën për ti mbrojtur dhe njohur ato;
- Unë e kuptoj se si veprimet e mia mund të cënojnë privatësinë e të tjerëve;
- Unë e kuptoj se si mbrojtja e privatësisë nuk është vetëm për jetën private të çdokujt, por mund të zbatohet gjithashtu në hapësirën publike, veçanërisht në internet;

Rezultatet e AFTËSIVE

- Unë mund të jap shembuj të situatave që i përkasin jetës private (p.sh. konsultimet mjekësore, ndarja prindërore);
- Unë vlerësoj se çfarë informacioni mund të përhap ose jo për veten time dhe të tjerët (p.sh. adresën e banimit, sëmundja e një të afërmi, etj.);
- Unë mund të jap shembuj të situatave në të cilat përdorimi i medias digjitale ka zgjeruar të shprehurit e lirive civile dhe/ose, në të kundërt, cunguar ato.

Të gjithë kemi gjëra që nuk duam t'i ndajmë me të tjerët.
Jo sepse është e paligjshme, por thjesht sepse është private.
Çfarë mendoni se është private?
Ndoshta ju njihni shumë njerëz...
A ndani pak gjëra me disa prej tyre, apo u tregoni çdo gjë të gjithëve?
Disa shpërndajnë pak gjëra, disa më shumë.

Të dyja veprimet janë të rregullta.
E njëjta gjë ndodh edhe në internet.
Imagjinoni të gjithë informacionin, fotot që njerëzit shpërndajnë në internet. Ndoshta jeni intervistuar nga gazeta lokale dhe ajo është e publikuar online. Nëse jeni anëtar i një ekipi sportiv, gazeta mund të ketë publikuar fotot e tua në faqen e saj.
Çfarë doni realisht që të tjerët të dinë rreth jush?
Organizata e Kombeve të Bashkuara deklaron se të gjithë fëmijët kanë të drejtën e privatësisë. Sa më i madh të jesh, aq më shumë mendimi yt duhet të merret parasysh. Për shembull, nëse nuk doni që prindërit të të publikojnë fotot, keni të drejtë të kundërshtoni. Dhe ky vendim duhet të respektohet.
A keni, gjithashtu, përgjegjësi? Kujtohuni, që e gjithë bota mund të shikojë informacionin dhe fotot që ju shpërndani. Për shembull, a do t'i varnit në muret e lagjes të njëjtat foto? Ose, do të shpërndanit informacion rreth shokëve tuaj tek të panjohurit? Ndoshta jo!
Kur je para kompjuterit, fotoja qesharake me miqtë mund të duket e padëmshme për t'u shpërndarë në rrjet. Por, nëse ju mendoni se ajo foto është qesharake, nuk do të thotë detyrimisht se miku juaj është dakord! Nëse doni të publikoni diçka për miqtë tuaj në internet, duhet të kërkoni fillimisht leje, ashtu si edhe të tjerët duhet të bëjnë të njëjtin veprim ndaj jush. Thjesht, miratoni, nëse mendoni se çdo gjë është në rregull.
Jeni ju ai që merr vendimet për privatësinë tuaj!Kjo është e drejta juaj, sepse është jeta juaj private!
Ndoshta ju nuk e dinit që ekzistojnë ligje dhe rregullore për këtë. Të njëjtat rregulla zbatohen kudo.
Mbroni privatësinë tuaj!

Ju vendosni!

Për t'u thelluar më shumë:

https://youtu.be/tysTgs3FIaM

[3/9] Kuptueshmëria e mjedisit digjital – aspektet teknike

Qëllimi: Për të mbrojtur privatësinë e tij/saj, studenti duhet të kuptojë mjedisin digjital dhe duhet të jetë i aftë të lundrojë në mënyrë të pavarur. Që të bëhet kjo, është e nevojshme të kuptohen sistemet hardware dhe infrastruktura teknike e sistemeve të informacionit që mbështesin shpërndarjen.

Rezultatet e NJOHURIVE

- Unë e di ndryshimin midis aplikacioneve *hardware dhe software;* unë e kuptoj se si **komponentët *hardware dhe software*** përbëjnë sistemet kompjuterike;
- Unë e di se çfarë janë **interneti dhe shërbimet e tij** (rrjetet sociale, aplikacionet telefonike, cloud, etj.);
- Unë e kuptoj se si është strukturuar hapësira digjitale (rrjetet fizike, browser, adresat IP dhe URLs, motorët e kërkimit, etj.);
- Unë jam i vetëdijshëm për konceptin e **arkitekturës** së informacionit, dhe mbledhjes, strukturës dhe përpunimit të informacionit;
- Unë e di **riskun kryesor të IT;** unë e di çfarë përfshin **siguria digjitale** dhe kuptoj nevojën për të siguruar sigurinë logjike dhe fizike të një mjedisi digjital.

Rezultatet e AFTËSIVE

- Unë i vlerësoj praktikat e mia dhe zhvilloj **zgjidhjen e problemit** dhe reflekset e **mësimit** – konkretisht rreth sigurisë – duke identifikuar burimet (komunitetet dhe forumet e përdoruesve, tutorialet, etj.);
- Unë mund të identifikoj funksionet e gabuara dhe të zgjidh probleme të thjeshta duke ndjekur procedurat e vendosura; nëse është e nevojshme, unë e di se si të kërkoj zgjidhje online, veçanërisht kur bëhet fjalë për sigurinë e mjedisit tim digjital.

PC, laptop, tablet

Ju duhet të jeni të parët që mbroni pajisjet tuaja kundër veprimeve me qëllime dashakeqëse. Përdoruesit e paautorizuar mund të instalojnë programe (viruse, worms, trojanë, spyware, etj) në kompjuterin tuaj nëpërmjet Internetit ose një email-i pa dijeninë tuaj. Programe të tilla mund të thyejnë të dhënat tuaja personale dhe kodet duke shkatërruar dosjet tuaja dhe programet dhe në përgjithësi dëmtojnë kompjuterin tuaj.

Risqet online

Keni dëgjuar në lajme, keni lexuar nëpër faqe Internet apo rrjete sociale për numra kartash krediti të vjedhura ose viruse që përhapen ne masë. Ndoshta edhe vetë keni qënë viktimë. Një nga mbrojtjet më të mira është të kuptoni rreziqet, cilat janë termat kryesor dhe si mund të mbroheni nga sulme të tilla.

Cilët janë rreziqet?

Ka mjaft rreziqe, disa janë të rëndë, disa më të lehtë. Ka ndër këta viruse që fshijnë totalisht sistemin tuaj, disa të tjerë futen në sistemin tuaj dhe ndryshojnë skedarët, disa viruse të tjerë përdorin kompjuterin tuaj për të sulmuar kompjutera ose sisteme të tjera, disa vjedhin informacionin tuaj të kartës së kreditit për të bëre blerje të paautorizuara. Fatkeqësisht nuk ka asnjëherë 100% garanci që edhe me aplikimin e masave më të mira të sigurisë gjëra të tilla nuk do të ndodhin, por me marrjen e këtyre masave ju mund të minimizoni mundësitë e një sulmi të mundshëm ndaj jush.

Mbroni paisjen tuaj me programe të sigurisë

– Firewalls
– Antivirus
– Antispyware

Jini të kujdesshëm dhe të "matur" duke përdorur Internetin

– Fshini dosjet e përkohshme që krijohen nga browser-i juaj i Internetit.
– Mos iu përgjigjeni email-eve te panjohura që kërkojnë për detajet e llogarisë tuaj bankare ose kodet e sigurisë.
– Mos injoroni "sjellje të çuditshme" të paisjes tuaj.
– Gjithmonë përditesoni sistemin tuaj të paisjes dhe programet që përdorni me versionet më të fundit.
– Gjithmonë i mbani kodet e sigurisë të sigurt.
– Shmangni përdorimin e rrjeteve, kompjuterave apo paisjeve të personave të tretë për përdorimin e WEB Banking.
– Kontaktoni me specialistë menjëherë në rast se ju dyshoni ndonjë përpjekje për vjedhjen e kodeve të sigurisë tuaj.

Rrjeti në shtëpi

Kur të krijoni një rrjet pa tela në shtëpi (wireless), sinjali broadband do të kalojë muret (shpërndahet rreth 100 metra) dhe do të jetë i ekspozuar edhe për personat e paautorizuar. Mbrojtja e rrjetit wireless është thelbësore në qoftë se ju dëshironi të mbani lidhjen tuaj private të sigurt.

Si mbrohet rrjeti pa tela?

Duhet të merren disa hapa:

Ndrysho fjalëkalimin fillestar për Router ose Access Point

Sapo të konfiguroni ndonjë WLAN, hapi i parë që duhet të bëni është të ndryshoni fjalëkalimin fillestar të router-it ose access point-it.

ÇFARË ËSHTË INTERNETI?

Interneti revolucionalizoi kompjuterat dhe botën e komunikimit si anjëherë tjetër më parë. Interneti ka filluar të zhvillohet në fund të viteve 1960 në Shtetet e Bashkuara të Amerikës. Interneti është sistem global i rrjetave të ndërlidhura kompjuterike të cilat bëjnë shkëmbimin elektronik të të dhënave (tekst, muzikë video, fotografi, etj) nëpërmjet përdorimit të kabllove te bakrit, fibrave optike, lidhjeve pa tela dhe teknologjive të tjera. Këto informacione mund të lexohen, shikohen apo shkarkohen nga përdoruesit e tjerë. Pra interneti mundëson praktikisht komunikimin nga një pajisje kompjuterike në tjetrën.

Disa nga shërbimet që interneti ofron aktualisht janë:

- Kërkimi në internet (WebBrowsing) – Ofron mundësi shfletimi në faqe të ndryshme nëpërmjet aplikacioneve kompjuterike të tilla si Google Chrome, Safari, Internet Explorer;
- Posta Elektronike (E-mail) - mundëson dërgimin e mesazheve të tipit tekst, foto, muzikë, video nga një person te një tjetër;
- Bisedat Online (Chat Online) – përdoren për të komunikuar në mënyrë të menjëhershme me personat që janë në linjë online;
- Rrjetet sociale (prsh . Facebook, Twitter, Instagram)
- Lojrat Online

Shërbimet e Internetit

Interneti është fantastik. Ju mund të bisedoni me miqtë tuaj në MSN, të shikoni filma në YouTube, të shkarkoni muzikë, të vizitoni faqet e miqve tuaj dhe të shpërndani fotot tuaja. Interneti ofron mundësi të pafundme për tu parë dhe dëgjuar.

Ishte ndryshe kur prindërit tuaj ishin të rinj. Në parim, duhej që ato të ishin të famshëm duke fituar çmime si futbollisti më i mirë i botës ose ndonjë çmim nobel për tu vënë re nga bota jashtë. Aktualisht, fotot që poston në Flickr ose video që vendos në YouTube, mund të shihen nga miliona njerëz – duke filluar nga gjyshja jote në një qytet tjetër, një hidraulik në Brazil, madje edhe nga bashkëshorti juaj i ardhshëm.

A keni menduar ndonjëherë nëse dëshironi që prindërit apo fqinjët tuaj të shikojnë se çfarë postoni në internet? Sepse ka shumë mundësi që ato të munden.
Në disa komunitete online, ju mund të vendosni se çfarë mund të shohin të tjerët në profilin tuaj. Por etiketimi, prerja dhe ngjitja janë të lehta në internet. Është shumë e lehtë që diçka që do të ndahej me miqtë e juaj, të shikohet edhe nga të tjerë dhe në çast që postohet, bëhet e vështir për të hequr.

Për t'u thelluar më shumë:

http://www.idp.al/wp-content/uploads/2016/11/broshur_smartphone.pdf

http://www.idp.al/wp-content/uploads/2016/10/fletepalosje_sugjerime_per_te_mbrojtur_privatesine_ne_internet.pdf

www.cyberalbania.al

www.isigurt.al

[4/9] Kuptueshmëria e mjedisit digjital – aspektet ekonomike

Qëllimi: Të kuptuarit e mjedisit digjital dhe lundrimi i tij në mënyrë të pavarur kërkon kuptueshmërinë e tij si një ekosistem dhe të kuptuarit e logjikës së tij; kjo përfshin njohurinë dhe kompetencat: ekonominë dhe vlerat e të dhënave personale, shërbimet dhe lojtarët kryesorë dhe modelet ekonomike.

Rezultatet e NJOHURIVE

- Unë e di se kush janë aktorët kryesorë në ekonominë digjitale (p.sh. ISPs, ofruesit e shërbimeve, zhvilluesit , etj.);
- Unë i kuptoj sistemet e përdorura për produktet e tregut dhe që ofrojnë **shërbimet e falas** (kartat e besnikërisë, reklamat nëpërmjet cookies, ngritjen e llogarive të përdoruesve, nënshkrimi në buletin, etj.), për qëllimin e vendosjes së **profileve të personalizuara të përdoruesve;**
- Unë e kuptoj se shumica e ofertave të tilla të shërbimeve detyron mbledhjen dhe përdorimin e të dhënave personale si edhe arkivimin e këtij informacioni në një bazë të dhënash;
- Unë e di se çfarë të dhënash janë mbledhur dhe arkivuar kur përdor internetin, një rrjet social apo një shërbim.

Rezultatet e AFTËSIVE

- Unë mund të jap shembuj të llojeve të të dhënave teknike që me shumë mundësi mblidhen kur unë jam online (p.sh. lloji i browser, lista e kontakteve, të dhënat e vendndodhjes, mesazhet private, etj.).
- Në çdo faqe interneti, unë mund të gjej **kushtet dhe kriteret e përdorimit** të të dhënave personale (kushtet dhe kriteret e përdorimit, informacioni ligjor, politikat e privatësisë, etj.).
- Unë mund të jap shembuj të shërbimeve digjitale modeli ekonomik i të cilave përfshin – ose jo – mbledhjen e të dhënave personale.

Me zhvillimin e teknologjisë dhe veçanërisht të Internetit vërehen disa zhvillime sa interesante aq edhe shqetësuese edhe në botën e medias. Lehtësia e madhe për të hapur një media digjitale nëpërmjet Internetit, si për shembull një gazetë elektronike, një kanal në Youtube ose edhe thjesht një blog informativ, i ka bërë njerëzit të mendojnë që mjafton kaq pak që të quhen gazetarë.

Si pasojë e kësaj vërejmë sot mundësi informimi të panumërta në Internet duke e pasur të vështirë dallimin e burimeve serioze dhe profesionale. Për këtë arsye është e rëndësishme të kihet kujdes edhe kur si mjet informimi përdoret një media digitale në Internet sepse jo vetëm mund të keqinformohemi por edhe mund të jemi viktima të njerëzve keqdashës që e përdorin atë mjet informimi për arsye krejt të tjera nga sa shfaqen.

- Mos i besoni asnjëherë verbërisht një informacioni të marrë në Internet.
- Përdorni më shumë se një burim për informimin tuaj.
- Lexoni politikat e privatësisë për të parë si përdoren të dhënat që mblidhen për ju, sa herë e vizitoni atë faqe informative.
- Mos komentoni apo dërgoni mesazhe fyese në faqet informative
- Përdorni vazhdimisht programe mbrojtëse për kompjuterin tuaj kur vizitoni faqe informuese

ÇFARË ËSHTË "SPAM"?

Spam, të njohur gjithashtu si"Junk Mail" është një nënbashkësi email, të cilët përfshijnë mesazhe pothuaj identike dhe jua dërgon disa marrësave me anë të postës elektronike e-mail. Përcaktimi i termit "spam" zakonisht përfshin aspektin qe emaili është i pakërkuar nga marrësi.
Shumë emaile"spam" përmbajnë URL të një websiti apo website.
Megjithatë, ia vlen të kujtohet që dërguesi në përgjithësi nuk ka objektiv marrësit personalisht. I njëjti e-mail "spam" mund të dërgohet në miliona njerëz në të
njëjtën kohë dhe adresat shpesh mund të jenë të hamendësuara. Personat (spammers) që dërgojnë "spam", mbledhin adresat e e-maileve nga dhomat e komunikimeve elektronike (chatrooms), website, lista e klientëve dhe viruset të cilat sulmojnë adresat e përdoruesit dhe ju shiten"spamersave" të tjerë.

Për t'u thelluar më shumë:

http://www.idp.al/wp-content/uploads/2016/11/broshur_informacion_mbi_spam.pdf

http://www.idp.al/wp-content/uploads/2016/11/broshura_cfare_eshte_marketingu_telefonik.pdf

[5/9] Kuptueshmëria e rregulloreve dhe legjislacionit të të dhënave personale

Qëllimi: Njohuria mbi sistemet e mbrojtjes së të dhënave dhe institucioneve mbulohet në këtë aftësim: parimet ligjore, tekstet e zbatueshme ligjore, autoritetet e mbrojtjes së të dhënave (DPA). Studenti kupton se në disa shtete, të dhënat personale mbrohen nga ligje dhe rregullore, që do të thotë se individët apo organizatat mund t'i përdorin ato në kushte dhe rrethana të caktuara.

Rezultatet e NJOHURIVE

- Unë e di se të dhënat personale nuk mund të përdoren për çfarëdo qëllim dhe se ekzistojnë rregulla për këtë;
- Unë i di dhe kuptoj **rregullat kyçe të mbrojtjes së të dhënave:**
    - Të dhënat personale përpunohen ose përdoren për qëllime specifike dhe duhet të kenë lidhje apo të jenë në përputhje me aktivitetin në fjalë (p.sh. qëllimi, proporcionaliteti);
    - Disa të dhëna sensitive të veçanta mund të jenë, në shtete të caktuara, të rregulluara në një mënyrë specifike (p.sh. të dhënat e minorenëve, origjina racore e njerëzve);
    - Të dhënat personale nuk duhet të mbahen më gjatë se është e nevojshme dhe duhet të arkivohen ose fshihen (periudha e mbajtjes) sipas ligjeve për mbrojtjen e të dhënave personale;
    - Njerëzit kanë të drejta lidhur me të dhënat e tyre personale (p.sh. qasje, korrigjim, refuzim, pëlqim);
    - Të dhënat personale mblidhen dhe përpunohen ose përdoren nën kushtet që sigurojnë privatësinë;
- Unë e di se organizatat private dhe publike që mbledhin dhe përpunojnë apo përdorin të dhëna personale duhet të kenë përputhshmëri me këto rregulla dhe se shkeljet mund të sjellin vendosjen **e sanksioneve, sipas shteteve;**
- Unë e di për ekzistencën, rolin dhe kompetencat e **Autoriteteve të Mbrojtjes së të Dhënave;**
- Unë e di se njerëzit për të cilët mblidhen të dhëna personale, duhet të informohen mbi të drejtat e tyre dhe se çfarë përdorimit do t'i bëhet dhe kujt do t'i shpërndahen të dhënat e tyre.

Rezultatet e AFTËSIVE

- Unë mund të jap shembuj të praktikave digjitale që mendoj se kanë **përputhshmëri** me dhe/ose **shkelin** rregulloret e mbrojtjes së të dhënave;
- Unë e njoh Autoritetin e Mbrojtjes së të Dhënave në vendin tim ose të jap një shembull të një Autoriteti të Mbrojtjes së të Dhënave dhe mund të citoj shembuj të veprimeve apo vendimeve të marra nga autoriteti;
- Nëse një Autoritet i Mbrojtjes së të dhënave ekziston në vendin tim, mund ta kontaktoj për këshillë dhe informacion.

TË DHËNAT PERSONALE DUHET TË PËRPUNOHEN NË MËNYRË TË DREJTË DHË TË LIGJSHME

Çfarë nënkuptohet me përpunim të drejtë?

Përpunimi i të dhënave personale duhet mbi të gjitha të jetë i drejtë, si dhe të plotësojë kushtet përkatëse për përpunim. "Përpunimi" përgjithësisht nënkupton grumbullimin, përdorimin, zbulimin, mbajtjen, ndreqjen, fshirjen, transmetimin, transferimin ndërkombëtar të të dhënave personale si dhe shkatërrimin e tyre.

Përpunimi i drejtë në përgjithësi kërkon transparencë me individët se si do të përdoren informacionet e tyre.

TË DHËNAT PERSONALE DUHET TË GRUMBULLOHEN PËR QËLLIME SPECIFIKE DHE TË LIGJSHME. TË DHËNAT NUK DUHET TË PËRPUNOHEN MË TEJ APO NË NDONJË MËNYRË TË PAPAJTUESHME ME KËTO QËLLIME

Kjo kërkesë ka për qëllim të sigurojë që kontrolluesit të jenë të hapur në lidhje me qëllimet për mbledhjen e të dhënave personale dhe se përdorimi i informacionit është në përputhje me këto qëllime.
Në praktikë, do të thotë se ju duhet të jeni të qartë që nga fillimi sepse i keni mbledhur të dhënat personale dhe atë që keni ndërmend të bëni me to.

TË DHËNAT PERSONALE DUHET TË JENË TË SAKTA DHE KUR ËSHTË E NEVOJSHME TË PËRDITËSOHEN

Ligji ka dispozitë të veçantë në lidhje me saktësinë e informatave që individët sigurojnë për veten e tyre, ose që japin për palët e treta. Për shembull, nëse një individ ka ndryshuar vendbanimin nga Durrësi në Tiranë, një regjistrim që tregon se ai aktualisht jeton në Durrës është padyshim i pasaktë. Por, një regjistrim që tregon se ai dikur ka jetuar në Durrës mbetet i saktë edhe pse ai nuk jeton më aty.

Për t'u thelluar më shumë:

http://www.idp.al/broshura-mbrojtja-e-te-dhenave-personale/

[6/9] Kuptueshmëria e rregullave të të dhënave personale: kontrolli i përdorimit të informacionit personal

Qëllimi: Studenti mësohet se përdorimi i kontrolluar i të dhënave të tij/saj personale është i nevojshëm dhe i ligjshëm, bazuar në kontekstin në të cilin përdoret në jetën e përditshme (si student, anëtar ekipi, anëtar familjeje, etj.). Mënyra që studenti identifikon veten e tij/saj dhe/ose e ben atë të njohur për të tjerët në botën digjitale mund të varet nga situata dhe t'i çojë ata në zbulimin e më shumë ose pak informacioni rreth vetes së tyre. Kjo është si të mësosh të manaxhosh "identitetin digjital". Studentët janë njohur gjithashtu me faktin që ata kanë të drejta dhe detyra, veçanërisht drejt të tjerëve.

Rezultatet e NJOHURIVE

- Unë e kuptoj nevojën dhe qëllimin e dhënies ose jo të informacionit personal, në varësi të kontekstit dhe qëllimi i përdorimit të tij;
- Me këtë qëllim, unë di të krijoj dhe përdor pseudonime dhe më shumë se një adresë e-maili, llogari dhe/ose profil **varur nga mënyra se si synoj ti përdor ato.**
- Unë e di se është e nevojshme të monitorojë rregullisht se çfarë thuhet online për mua (reputacioni im);
- Unë e di se publikimi kërkon marrjen e **përgjegjësisë për pjesën time** dhe atë të prindërve të mi/ kujdestarëve ligjorë.

Rezultatet e AFTËSIVE

- Unë jam i kujdesshëm të shpërndajë vetëm të dhënat personale që janë absolutisht të nevojshme për t'u regjistruar për një shërbim;
- Unë mund ta shpreh veten time *online* duke marrë parasysh **natyrën e hapësirës** ku po publikoj (hapësirë private, publike, lidhur me shkollën, familjen, miqtë, etj.);
- Unë jam **vigjilent për ato që publikoj *online,*** edhe nën një **pseudonim;**
- Unë mund të marrë pjesë në një debat online me ***respekt për të tjerët:*** unë nuk shpërndaj informacion dhe foto të palëve të treta pa informimin e tyre dhe se mund të dëmtojnë privatësinë dhe reputacionin e tyre;
- Unë përdor mjete për të monitoruar rregullisht përmbajtjen dhe informacionin për mua që shikohet nga të tjerët në rrjetet sociale.

Fjalëkalimet

Një nga mënyrat më të mira për të mbrojtur të dhënat tuaja personale është që të siguroni se vetëm njerëzit e autorizuar të kenë akses në to. Verifikimi se dikush është personi që pretendon të jetë është hapi tjetër, dhe ky proces autentifikimi është edhe më i rëndësishëm, dhe më i vështirë, në botën kibernetike.

Fjalëkalimet janë mjetet më të zakonshme të autentifikimit, por nëse ju nuk zgjidhni fjalëkalime të mira apo ti mbani ato konfidenciale, ato janë pothuajse aq të paefektshëm sa mos të paturit fjalëkalim. Shumë sisteme dhe shërbime janë thyer me sukses për shkak të përdorimit të fjalëkalimeve të pasigurta dhe të pamjaftueshme, dhe disa viruse dhe krimba kanë shfrytëzuar sisteme nga hamendësimet e fjalëkalimeve të dobëta.

Si mund të zgjidhni një fjalëkalim të mirë?

Edhe pse qëllimisht ta shkruash keq një fjalë ("daytt" në vend të "data") mund të ofroj një mbrojtje kundër sulmeve , një metodë edhe më e mirë është që të përdoresh në një seri fjalësh dhe të përpiqesh t'i kujtosh në çdo kohë. Për shembull, në vend të fjalëkalimit "hoops," përdorni "UpTlbb" për "[U]ne [p] elqej [T]e [l]uaj [b]asket[b]oll".

Duke përdorur shkronja kapitale dhe jokapitale i shton një tjetër shtresë errësire fjalëkalimit. Mbrojtja juaj më e mirë, megjithatë, është të përdorni një kombinim numrash, karakteresh të veçanta, dhe të dy llojet e shkronjave kapitale dhe jokapitale.

Për t'u thelluar më shumë:

http://www.idp.al/broshura-mbrojtja-e-te-dhenave-personale/

[7/9] Menaxhimi i të dhënave të mia: të mësuarit për ushtrimin e të drejtave të mia

Qëllimi: Këtu ne mësojmë për rrethin e veprimeve të mundshme për mua si një fëmijë/adoleshent kur vjen puna tek pëlqimi apo refuzimi i mbledhjes së të dhënave të mia personale, njoftimit, raportimit dhe mbrojtjes së vetvetes – nëpërmjet ndërhyrjes nga një i rritur, kur është e përshtatshme (*) – për tu përballur me situatat të provuara dhe/ose të identifikuara për prishjen e privatësisë dhe/ose integritetin e personave, ose që përbëjnë shkelje të ligjit.
(*) duke prezantuar konceptin e ndërhyrjes nga një i rritur përgjegjës dhe/ose kujdestar ligjor, autorët marrin në konsideratë specifikat e legjislacionit kombëtar, shërbimet e ofruara, grupmoshat, nivelin autonom të fëmijëve dhe praktikat e identifikuara.

Rezultatet e NJOHURIVE

- Unë e di se, për të përdorur shërbime të caktuara *online,* **kërkohet** pëlqimi im apo i prindërve/kujdestarëve të mi
- Unë e di se kam të drejta lidhur me të dhënat personale (p.sh. qasje, korrigjim, refuzim, pëlqim, delistim, fshirje) dhe se mund ti ushtroj këto të drejta në emrin tim duke kontaktuar shërbimin në fjalë sipas procedurave të brendshme dhe në rast refuzimi apo ndonjë problemi, duke kontaktuar Autoritetin e Mbrojtjes së të Dhënave, një gjykatës sipas shteteve dhe/ose autoritetet relevante kombëtare/nën-kombëtare, apo grupet e mbrojtjes.

Rezultatet e AFTËSIVE

- Unë mund të përditësoj ose kërkoj përditësime për të dhënat lidhur me mua që duket të jenë **vjetërsuara, të pasakta ose të paplota,** nëse është e nevojshme.
- Unë mund të kërkoj fshirjen e të dhënave të mia personale online;
- Unë jam i aftë të kontrolloj me shërbimin në fjalë nëse janë mbledhur dhe arkivuar, ose jo, të dhëna personale në **një bazë të dhënash (database).** Nëse është e nevojshme, unë mund ta marr këtë informacion nga shërbimi në fjalë dhe të ushtrojë- ose të kem ushtruar në emrin tim – të drejtat e tjera në lidhje me shërbimin në fjalë;
- Unë jam i aftë të dal nga një shërbim dhe ose të fshijë një llogari që kam krijuar.

KONVENTA E KOMBEVE TË BASHKUARA MBI TË DREJTAT E FËMIJËVE THOTË:

- Asnjë fëmijë nuk do të jetë subjekt i ndërhyrjeve të paligjshme apo të paarsyeshme në privatësinë e tij apo saj, familjen, korrespondencën, ndaj sulmeve të paligjshme mbi reputacionin dhe nderin e tij apo të saj.
- Palët e Shteteve do të sigurojnë fëmijës që është i aftë në formimin e pikëpamjeve të tij apo të saj, të drejtën për ti shprehur ato të drejta lirisht në të gjitha çështjet që cenojnë fëmijën.

Por Konventa e Kombeve të Bashkuara mbi të Drejtat e Fëmijëve thotë gjithashtu se: të dy prindërit kanë një përgjegjësi parësore për kujdesin e fëmijës dhe zhvillimin sipas asaj që është më e mira për të. Prandaj prindërit duhet t'iu mbrojnë kur diçka ju cenon ju. Nëse ata mendojnë se ju po bëni diçka në internet që është e dëmshme për ju dhe të tjerët, ata mund të vendosin kufij për ato që mund të bëni.

BISEDIMI ME FËMIJËT

Mënyra më e mirë për t'i mbrojtur fëmijët në internet? Flisni me to. Ndërkohë që fëmijët vlerësojnë opinionet e bashkëmoshatarëve të tyre, shumica priret të mbështetet tek prindërit e tyre për ndihmë mbi problemet që kanë më shumë rëndësi.

Fëmijët shikojnë prindërit e tyre që përdorin të gjitha llojet e pajisjeve duke luajtur lojëra apo shikuar shfaqje në to. Në momentin që fëmija fillon të përdorë një telefon, pajisje telefoni apo kompjuter, është koha për të biseduar me to rreth sigurisë dhe sjelljes në internet. Edhe nëse fëmijët afrohen me ju, mos prisni që ata të fillojnë bisedën. Shfrytëzoni mundësitë e përditshme për të biseduar me fëmijët rreth internetit. Për shembull, histori të reja për bullizmin kibernetik apo mesazhet ndërsa i jepni makinës mund të nxisë një bisedë me fëmijët rreth eksperiencave të tyre dhe pritshmërie tuaja.

Për t'u thelluar më shumë:

http://www.idp.al/broshura-mbrojtja-e-te-dhenave-personale/

[8/9] Menaxhimi i të dhënave të mia: të mësuarit për të mbrojtur veten *online*

Qëllimi: Ky parim mbulon zgjidhjet e përdorura për të siguruar mbrojtjen teknike dhe sigurinë e të dhënave personale. Këto zgjidhje janë subjekt i proceseve të të mësuarit brenda kuadrit kolektiv të shkollës dhe mjediset e saj. Studentët duhet të dinë se si të përdorin pajisjet teknike për të identifikuar dhe vërtetojnë vetveten online, të autorizojnë ose jo mbledhjen e të dhënave personale, dhe të krijojnë një llogari dhe/ose profil në përputhje me rregullat e mbrojtjes së të dhënave.

Rezultatet e NJOHURIVE

- Unë e di se ka **mënyra për ta mbrojtur veten *online:*** në veçanti, unë njihem me mënyra të ndryshme për të identifikuar dhe vërtetuar veten time. Jam i vetëdijshëm për zgjidhjet e enkriptimit të të dhënave;
- Unë i kuptoj kushtet dhe kriteret e përdorimit në lidhje me shërbimet online (lejo ose refuzo vendndodhjen, lejo ose refuzo aksesin e aplikacioneve tek kontaktet e mia, fotot, etj.);
- Unë e di se mund të **menaxhoj konfigurimet** e aplikacioneve online dhe shërbimeve që përdor.

Rezultatet e AFTËSIVE

- Unë përdor procedura të disponueshme për të mbrojtur të dhënat e mia personale: për llogaritë e mia dhe profilet mund të krijoj fjalëkalime të sigurta, apo parafrazime dhe i ndryshoj ato rregullisht; unë mund të ekzaminoj dokumente dhe foto që shpërndaj në internet dhe nëse është e nevojshme, mund të përdor mjete për të fshirë metadata; dhe zgjidhjet e enkriptimit të të dhënave;
- Mund të menaxhoj **sigurinë dhe konfigurimet e privatësisë** të llogarive, profileve dhe pajisjeve që përdor; i **kontrolloj shpesh** këto konfigurime dhe i **ndryshoj ato.**

Krijoni profilin me email të veçantë

Nëse vendosni të hapni një profil në një rrjet social atëherë përdorni një email të veçantë vetëm për këtë shërbim dhe fjalëkalimin tuaj mos ia jepni askujt tjetër. Gjithashtu vendosni opsionin e gjuhës në shqip në rast se keni probleme me gjuhën.

Njihuni me dokumentet e rrjetit social

Përpara se të përfundoni procesin e hapjes së një llogarie në rrjetit social lexoni mirë "Kushtet e Përdorimit" dhe "Politikën e Privatësisë". Për të lexuar këto karta mjafton të klikoni te lidhjet përkatëse në fund të faqes së regjistrimit përpara se të kryeni këtë veprim. Gjithashtu një element tjetër i rëndësishëm është ndjekja e përditësimit të "Politikës së Privatësisë" të rrjetit social.

Mendohuni mirë përpara se të pranoni një kërkesë për shok

Pasi ju pranoni dikë të bëhet shoku juaj ai do të jetë në gjendje të ketë akses në informacionet tuaja si fotot apo kontaktet. Ju mund të hiqni shokët tuaj në çdo kohë nëse mendoni se dikush nuk mund të jetë aq i ngushtë me ju ose mund të përdorni opsionet e mëposhtme duke kufizuar aksesin e tyre.

a) **Kuptoni kategorizimin e shokëve tuaj:** Kategorizmi i shokëve në **rrjetin social** është themel i privatësisë së këtij shërbimi. Koncepti i këtij opsioni është se ju mund të organizoni dhe kategorizoni shokët në grupe të veçanta. Një listim tipik është ai i grupimit në **kategori shok, familje** dhe **profesionale.** Kjo bën të mundur aksesin e të dhënave tuaja në bazë të privilegjeve të çdo grupi. Si p.sh fotot që publikoni për familjen nuk mund të shihen nga grupi i shokëve në kategorinë profesionale. Ju mund të konfiguroni këtë kategorizim në hapësirën "shokët". Mos harroni të vendosni çdo shok të ri në kategori të paracaktuara sepse ndryshe ai nuk kategorizohet automatikisht.

b) **Bëni të gjitha opsionet jo aktive:** Mendoni se si dhe për cilat arsye ju dëshironi të përdorni **rrjetin social.** Nëse është thjesht për të pasur mundësinë e kontaktit me shokët atëherë është mirë që të hiqni shumë nga opsionet si ato të përshkruara në vazhdim. Është më mirë të hiqni një opsion deri sa të vendosni që ai ju nevojitet se sa të keni çdo gjë të hapur për të gjithë.

c) **Hiqni veten tuaj nga rezultatet e kërkimit:** Ka shumë arsye për të cilat individët nuk duan që informacionet e tyre të shfaqen në rezultatet e kërkimit në **rrjetin social** apo jashtë tij. Për shembull, duke kërkuar në Google me emër e mbiemër shfaqet foto e profilit tuaj, lista e shokëve tuaj dhe një listë e faqeve të Facebook të cilat ju i keni nënshkruar si adhurues. Që të bëni të shmangshme këto kërkime është një ide e mirë që të hiqni mundësinë e gjetjes së profilit tuaj dhe në faqen "rregullo privatësinë" te "llogaria" në opsionin "kërkoni" ju duhet të hiqni opsionin lejo "gjetjen në rezultatet e kërkimit publik".

d) **Bëni informacionin e kontakteve private:** Pasi pranoni një kërkesë të një "shoku" nga njerëz të cilët nuk i njihni, duhet që të merrni në konsideratë dukshmërinë e kontakteve tuaja. Mënyra më e mirë është që ju të vendosni një kufizim se kush mund të shohë kontaktet tuaja. Kjo bëhet duke klikuar tek "informacionet e kontaktit" Tek "rregullo privatësinë" dhe aty vendosni për secilën të dhënë nivelin e dukshmërisë.

Mbroni fotot dhe albumet tuaja

Është e rëndësishme që ju të mendoni se cilët janë personat të cilët dëshironi që të shohin fotot dhe albumet tuaja. Në "rregullo privatësinë" ju jeni në gjendje të ndani dukshmërinë e albumeve tuaja në mënyrën e dëshiruar. Madje ju mund të përzgjidhni çdo foto dhe ta kategorizoni atë në bazë të dukshmërisë.
Kjo mundëson për çdo njeri të mos arrijë të shohë foto apo video ku ju mund të jeni të etiketuar. Gjithsesi shumë përdorues dëshirojnë që shokët e tyre të shohin foto ku ata janë etiketuar e nëse jeni nga këta atëherë zgjidhni opsionin e duhur.
Se cilat opsione zgjidhni ju rreth privatësisë është vendim personal, por nëse doni të kufizoni aksesin e albumeve tuaja, atëherë ne ju rekomandojmë të bëni modifikimet e përshtatshme tek "foto dhe videot e mia" dhe "albumet e fotove" tek "preferencat e privatësisë".
Aty ju mund të kufizoni aksesin e secilit album sipas preferencave si psh. duke përzgjedhur "vetëm shokët".
Por mënyra më e mirë për të arritur një kompromis është nëpërmjet krijimit të kategorive të cilat u sugjeruan në fillim.

Kontrolloni aksesin e aplikimeve të informacionit

Kur ju vizitoni aplikimet e ndryshme të cilat ofrohen nga faqja e rrjetit social ato mund të përdorin informacionet tuaja që janë publike. Informacionet publike përfshijnë emrin, foton e profilit, gjininë, qytetin e banimit, rrjetin shoqëror, listën e shokëve dhe faqet e të cilave jeni adhurues.

Sa më të ngushta të bëni informacionet publike të profilit, më pak informacion bëhet i disponueshëm për aplikimet. Ndërkohë që aplikimet ndjekin preferencat tuaja të privatësisë, shokët tuaj mund të ndajnë informacione rreth jush nëpërmjet këtyre aplikimeve. Ju mund të modifikoni dhënien e këtij informacioni duke shkuar tek "preferencat e privatësisë" tek "aplikimet dhe faqet e internetit" dhe duke ç'aktivizuar opsionet që dëshironi të bëni jo publike tek "çka mund të ndajnë shokët tuaj me të tjerët rreth teje".

Për t'u thelluar më shumë:

http://www.idp.al/broshura-mbrojtja-e-te-dhenave-personale/

[9/9] Bota digjitale: Të bëhesh një qytetar digjital

Qëllimi: Studentët do të zhvillojnë një qasje kritike dhe etike për të lundruar mjedisin digjital me konfidencë dhe qartësi dhe të veprojnë me përputhshmëri. Duke i ushtruar këto të drejta, përdorimi i shërbimeve digjitale ndërsa respektohet mbrojtja e të dhënave personale, identifikimi ofruesve të shërbimit që mund të cenojë privatësinë ose liritë, raportimin, mobilizimin; të gjitha veprimet që përcaktojnë një qytetar digjital, përgjegjës për të dhënat e tyre dhe respektimin për të dhënat e të tjerëve.

Rezultatet e NJOHURIVE

- Mund të krahasoj informacionin dhe **vlerësoj nëse është apo jo i besueshëm;**
- Mund të analizojë dhe të vlerësoj në mënyrë kritike një situatë lidhur me përdorimin e medias digjitale (p.sh. përhapja e informacionit të rremë dhe/ose thashethemet);
- Mund të identifikoj përmbajtje dhe sjellje ilegale apo të papërshtatshme;
- Mund të njoh situata që përfshijnë dëmtimin e reputacionit apo **ngacmime kibernetike.**

Rezultatet e AFTËSIVE

- Në situatat e përshkruara më lart, unë mundem në mënyrë të drejtpërdrejtë apo nëpërmjet një të rrituri, **të njoftoj autoritetet dhe/ose shoqëritë e mbrojtjes;**
- Jam i aftë të nxis rezultate pozitive (i aftë të adresoj ankesa të cilat mund të influencojnë lojtarët e mëdhenj të internetit, ndërmjetësim për të siguruar që të ndalet sjellja e papërshtatshme, zhvillimi i kodeve të sjelljes, etj.);
- Jam i aftë të gjykoj nëse është e **përshtatshme** të publikosh informacion të tillë **në një kontekst të caktuar;** mund të analizoj dhe parashikoj pasojat potenciale të shpërndarjes në internet.

Rrjetet sociale si Facebook, Instagram dhe Snapchat janë ndër faqet më të përdorura në internet. Përdorimi i këtyre faqeve shtohet në mënyrë eksponenciale çdo ditë. Bashkë me këto rritje të përdorimit, shtohen edhe problemet e sigurisë kompjuterike lidhur me të. Një nga problemet ndoshta më të shpeshta të kësaj natyre është ai i krijimit të profileve të rremë. Rrjetet sociale mbajnë një politikë të saktë në lidhje me profilet e rreme. Sipas tyre realizohet fshirja e një profili të rremë pasi stafi e konstaton një gjë të tillë. Duhet thënë gjithsesi se gati të gjitha rastet kur ky fenomen ndodh, ai realizohet nga persona të njohur apo nga individ keqdashës. Nuk është rastësi që personat e famshëm gjenden shpesh me profile të pafundme në rrjete sociale edhe kur vetë ata nuk kanë hapur ende një të tillë.

Por abuzimet shkojnë përtej, pasi nëpërmjet profilit personi keqbërës fillon shtiret dhe komunikon me persona të tjerë sikur të ishte ai i vërtetë. Në këto rrethana dëmet janë së pari morale por dhe ndonjëherë më të ndërlikuara.

Kur ndodhin këto probleme mënyra mbase më e shpejtë dhe efikase e zgjidhjes së problemit është që personi i dëmtuar të kontaktojë direkt me rrjetin social duke kërkuar fshirjen e profilit të rremë.

Një mënyrë efiçiente për të realizuar këtë është me ndihmën e përdoruesve të tjerë të rrjetit social të cilët nëpërmjet një opsioni kanë mundësinë të raportojnë profilin e rremë. Në këtë kontekst duhet thënë se sa më shumë përdorues të rrjetit social (miq të atij të vërtetit) raportojnë aq edhe me e shpejtë mund të jetë përgjigja dhe konstatimi nga ana e stafit të vetë rrjetit social. Investigimi dhe kontrolli në sistemin e rrjeteve realizohet vetëm nga stafi i Facebook por mund të hetohet edhe nga institucione të autorizuara si policia, prokuroria, etj.

Duhet të sqarojmë që rrjeti social regjistron çdo lloj veprimi që kryhet nëpërmjet një profili dhe gjithashtu mban rekorde në lidhje me burimin dhe gjendjen fizike nga ku kryhen këto veprime. Kjo bëhet e mundur nëpërmjet monitorimit të adresave IP (Internet Protocol) nga ku vijnë kërkesat dhe nga ku kryhet aksesi. Duhet thënë që këto informacione nuk përcillen përgjithësisht tek ndonjë individi edhe nëse është vërtetuar se ka pasur vjedhje identiteti apo shkelje të tjera të reklamuara nga individi i dëmtuar. Këto rrethana krijojnë kushte shumë të vështira për një person të dëmtuar që të pajisjet më provat e nevojshme pranë një institucioni ligjor për të kërkuar dëmshpërblim apo drejtësi kundër personit që ka kryer veprën e falsifikimit të profilit.

SI TË MBROHEMI NGA PROFILET E RREMË

- Kini kujdes nga profilet fallco. Mjafton një foto, emri dhe disa informacione për jetën e një personi për të poseduar online identitetin e tij. Janë shumë tashmë rastet e aktorëve, politikanëve, personave publik, por edhe të njerëzve të zakonshëm që kanë gjetur në rrjetet sociale dhe në blog-e identitetin e tyre të menaxhuar nga të tjerë.

- Nga ana tjetër jo gjithmonë flitet, chat-ohet dhe ndahet informacione me ata që mendohet. Ai që mund të shfaqet si fëmijë mund të jetë një i rritur dhe e kundërta. Gjithmonë e më shumë krijohen identitete fallco (si të personazheve të famshëm, si të personave të thjeshtë) thjesht për lojë, për të mërzitur dikë apo për të kuptuar informacione të rezervuara. Mjafton fotoja jote dhe disa informacione mbi jetën tënde ... dhe i "klonuari" i ardhshëm mund të jesh ti.

- Gjithashtu, kur subjekti i të dhënave vendos vetë të dhënat personale në një rrjet social humbet kontrollin e tyre. Të dhënat mund të regjistrohen nga të gjitha kontaktet dhe nga pjesëtarët e grupeve tek të cilat është anëtarësuar, të ripunohen dhe të shpërndahen dhe në distancë vitesh.

- Duhet të dihet se pjesa më e madhe e faqeve të rrjeteve sociale kanë seli jashtë Shqipërisë dhe Evropës, po kështu edhe serverat e tyre. Për këtë shkak konfliktet me rrjetet sociale jo gjithmonë mund të zgjidhen nga legjislacioni shqiptar apo ai evropian.

- Prandaj Mbrojtësi më i mirë i privatësisë tënde je ti.

- Reflekto mirë para se të vendosësh online të dhëna që nuk dëshiron që të përhapen ose që të përdoren në dëmin tënd. Mendo mirë para së të publikosh të dhënat e tua personale (mbi të gjitha emrin, adresën, numrin e telefonit) në një profil përdoruesi, apo të pranosh me lirshmëri kërkesat për miqësi. Mbaj parasysh që fotot dhe informacionet e vendosura dikur mund të rishfaqen fal motorëve të kërkimit në distancë vitesh. Mos publiko informacione personale dhe foto të të tjerëve pa pëlqimin e tyre, se në këtë rast mbi ankimin e të dëmtuarit nga veprimet e tua të kundërligjshme mund të përgjigjesh penalisht sipas Kodit Penal të Republikës së Shqipërisë.

- Lexo mirë gjithë kontratën dhe kushtet e përdorimit të cilat i pranon kur regjistrohesh në një rrjet social. Kontrollo edhe modifikimet që bëhen/futen në mënyrë njëanshme nga ndërmarrja të cilat mund të bëhen në çdo kohë. Verifiko nëse mund të dalësh lehtë nga shërbimi dhe të mund të fshish të gjitha informacionet që ke publikuar mbi identitetin tënd.

Për t'u thelluar më shumë:

http://www.idp.al/broshura-mbrojtja-e-te-dhenave-personale/

Të bisedosh me fëmijët për përdorimin e Internetit – Këshilla për prindërit[2]

Njerëzit e të gjitha moshave po: komunikojnë me miq dhe familjen në internet; shkarkojnë aplikacione; ndajnë veprimtarinë dhe vendndodhjen e tyre; shpërndajnë foto dhe video nga pajisjet celulare; krijojnë reputacione dhe profile në internet.

Komunikimi në internet është një mënyrë jetese, por që përmban disa rreziqe:

Sjellje të papërshtatshme

Bota në internet mund të duket anonime. Ndonjëherë, fëmijët e harrojnë që janë akoma të përgjegjshëm për veprimet e tyre.

Kontakte të papërshtatshme

Disa njerëz në internet kanë qëllime të këqija. Ato mund të jenë bullistë, grabitqarë, hakerë apo mashtrues.

Përmbajtje e papërshtatshme

Ju mund të shqetësoheni se fëmijët tuaj mund të gjejnë pornografi, dhunë apo gjuhën e urrejtjes në internet.

Teknologjia po evoluon në mënyrë konstante. Po ashtu dhe rreziqet që shoqërohen me të. Mund ti reduktoni këto rreziqe duke biseduar me fëmijët tuaj për mënyrën se si ato komunikojnë në internet dhe jashtë tij dhe t'i nxisni ato që të mendojnë në mënyrë kritike dhe të veprojnë në atë mënyrë që të mund të ndjehen krenarë.

Ky udhëzues nga Komisioni Federal i Tregtisë të Shteteve të Bashkuara të Amerikës mbulon çështje për fëmijët rreth mënyrës së të vepruarit në internet.

BISEDIMI ME FËMIJËT TUAJ

Mënyra më e mirë për t'i mbrojtur fëmijët në internet? Flisni me ato. Ndërkohë që fëmijët vlerësojnë opinionet e bashkëmoshatarëve të tyre, shumica priret të mbështetet tek prindërit e tyre për ndihmë mbi problemet që kanë më shumë rëndësi.

[2]Ky material është përkthyer nga botimi I Autoritetit Federal të Tregtisë të Sh.B.A Në original titulli "Net Cetera – Chatting with Kids about being Online"

Filloni herët.

Fëmijët e vegjël shikojnë prindërit e tyre që përdorin të gjitha llojet e pajisjeve duke luajtur lojëra apo shikuar shfaqje në to. Në momentin që fëmija juaj fillon të përdorë një telefon, pajisje telefoni apo kompjuter, është koha për të biseduar me to rreth sigurisë dhe sjelljes në internet.

Filloni të bisedoni.

Edhe nëse fëmijët afrohen me ju, mos prisni që ato të fillojnë bisedën. Shfrytëzoni mundësitë e përditshme për të biseduar me fëmijët rreth internetit. Për shembull, histori të reja për bullizmin kibernetik apo mesazhet ndërsa i jepni makinës mund të nxisë një bisedë me fëmijët rreth eksperiencave të tyre dhe pritshmërie tuaja.

Komunikoni pritshmëritë tuaja.

Jini të sinqertë për pritshmëritë tuaja dhe se si aplikohen në internet. Komunikimi i qartë i vlerave tuaja, mund t'i ndihmojë fëmijët tuaj të marrin vendime më të arsyeshme dhe inteligjente kur hasin situata të vështira. Për shembull, jini specifik për atë që është jashtë limiteve dhe çfarë konsideroni të jetë sjellje e papranueshme.

Jini të durueshëm dhe përkrahës.

Mos nxitoni nëpërmjet bisedimeve me fëmijët tuaj. Shumica e fëmijëve kanë nevojë ta dëgjojnë disa herë informacionin, me doza të vogla që të ngulitet mirë në mendjen e tyre. Nëse vazhdoni të flisni me fëmijët tuaj, durimi dhe këmbëngulja do të shpërblehet më vonë.

Punoni shumë që të mbani hapur linjat e komunikimit, edhe nëse zbuloni që fëmija juaj ka bërë diçka të papërshtatshme.

Dëgjimi dhe marrja në konsideratë e ndjenjave të tyre ndihmon bisedën që të vazhdojë. Mund të mos i keni të gjitha përgjigjet, dhe të jesh i sinqertë për atë që mund të ketë një rrugëtim të gjatë.

KOMUNIKIMI NË MOSHA TË NDYSHME

Fëmijët e vegjël

Mbikëqyrja është e rëndësishme.

Kur fëmijë e vegjël fillojnë të përdorin telefonat apo një kompjuter, duhet të mbikëqyren afër nga një prind apo kujdestar. Nëse fëmijët e vegjël nuk mbikëqyren në internet, ato mund të pengohen në përmbajtjen që mund t'i frikësojë apo ngatërrojë ato.

Kur jeni komod në momentin që fëmijët tuaj mund të eksplorojnë vetë, është akoma e rëndësishme që të qëndroni afër tyre. Mund të dëshironi të ndaloni aksesin në faqe apo aplikacione që keni vizituar dhe që e dini se janë të përshtatshme – të paktën në kuadër të vlerave argëtuese dhe edukuese të tyre.

Konsideroni kontrollin prindëror.

Nëse jeni të shqetësuar për atë që shohin fëmijët tuaj në internet, merrni parasysh mjete me këto karakteristika:

- Filtrimi dhe bllokimi. Këto mjete limitojnë *aksesin* në faqe, fjalë apo foto të caktuara. Disa faqe interneti vendosin se çfarë filtrohet; disa të tjerë ja lënë prindërve. Disa filtra aplikohen për *website-t;* të tjerat për email-in dhe *chat-in.*
- Bllokimi i përmbajtjes. Ky *software* parandalon fëmijët në shpërndarjen e informacionit në internet apo nëpërmjet email-it.
- Koha e limituar. Ky software ju lejon të limitoni kohën e shpenzuar në internet të fëmijëve tuaj si edhe të caktosh kohën në të cilën ato mund të *aksesojnë* internetin.
- Browsers për fëmijë. Këto *browser* filtrojnë fjalë apo foto që nuk doni të shihen nga fëmijët tuaj.
- Motorë kërkimi të orientuara për fëmijë. Këto performojnë kërkime të limituara apo rezultate kërkimi të filtruara për faqe dhe materiale të përshtatshme për fëmijë.
- Monitorimi i mjeteve. Software që njoftojnë prindërit për aktivitetin *online* pa bllokuar *aksesin.* Disa mjete regjistrojnë adresat e website-ve që janë vizituar nga një fëmijë; të tjera japin një mesazh paralajmërues kur fëmijët vizitojnë faqe të caktuara. Mjetet monitoruese mund të përdoren me apo pa dijeninë e fëmijëve.

Binjakët

Binjakët kanë nevojë të ndjehen "të pavarur" por jo vetëm ndërkohë që fillojnë të eksplorojnë vetë. Shumë 8-12 vjetarë janë të aftë në gjetjen e informacionit, por që kanë nevojë për udhëzime për të kuptuar se cilat burime janë të besueshme.

Mendoni për limitet.

Konsideroni vendosjen e limiteve për kohën dhe shpeshtësinë që ato mund të jenë online – qoftë në kompjuter, telefon apo pajisje të tjera. Për adoleshentë më të rinj, kontrollet prindërore mund të jenë efektiv. Gjithsesi, shumë fëmijë kanë njohurinë teknike për të marrë situatën në dorë në këto kontrolle.

Adoleshentët

Adoleshentët po krijojnë vetë vlerat e tyre dhe po fillojnë të marrin ato të moshatarëve të tyre. Shumë prej tyre janë të gatshëm të kenë më shumë pavarësi nga prindërit e tyre. Gjithsesi, ato duhet të mësojnë se si të ushtrojnë gjykimin e të qenit të sigurt *online* dhe të veprojnë në dakordësi me etikën e familjes së tyre.

Adoleshentët kanë më shumë *akses* në internet nëpërmjet pajisjeve telefon- si edhe më shumë kohë për veten – pra nuk është realiste që të qëndroni në të njëjtën dhomë kur ato janë *online.* Ato kanë nevojë të dinë se ju dhe anëtarë të tjerë të familjes mund ti pyesë ato se çfarë po bëjnë *online.*

ÇFARË MUND TË BËNI?

Flisni për kredibilitetin.

Është e rëndësishme të theksohet koncepti i kredibilitetit. Edhe fëmijët më të kujdesshëm kanë nevojë ta kuptojnë:

- Jo çdo gjë që shikoni në internet është e vërtetë

- Njerëzit *online* mund të mos jenë ato që duken apo thonë.
- Informacionet dhe fotot që shpërndahen mund të shihen në pikëpamje të ndryshme
- Në momentin që diçka postohet *online* është thuajse e pamundur për "ta marrë mbrapsht"

Flisni për mënyrat.

Për shkak se ato nuk shohin shprehjet e fytyrës, gjuhën e trupit, dhe shenja të tjera vizuale, adoleshentë dhe binjakët mund të ndjehen të lirë të bëjnë apo thonë gjëra online që s'mund t'i thonë *offline.* Kujtojini atyre se njerëzit real me ndjenja reale janë pas profileve, emrave të ekranit dhe avatarëve.

Flisni për pritshmëritë.

Kur flisni për fëmijët, vendosni pritshmëri të arsyeshme. Parashikoni se si do të reagonit ju nëse do të zbulonit diçka që ato kanë bërë *online* dhe ju nuk do të aprovonit.

Nëse fëmija juaj beson tek ju për diçka të frikshme apo të papërshtatshme që kanë hasur *online,* përpiquni të punoni bashkë për ta parandaluar atë herë tjetër.

SOCIALIZIMI ONLINE

Fëmijët publikojnë foto, video, mendime, plane dhe vendndodhjen me miq, familjen dhe ndonjëherë me botën mbarë. Socializmi *online* mund t'i ndihmojë fëmijët të lidhen me të tjerët, por është e rëndësishme të ndihmoni fëmijën tuaj që të mësojë se si të lundrojnë në mënyrë të sigurt këto hapësira.

SHPËRNDARJE MASIVE

Disa gracka që vijnë me socializimin *online* po shpërndarjen e shumë informacioneve, apo postimin e fotove, videove ose fjalëve që mund të cenojnë një reputacion apo të dëmtojë ndjenjat e dikujt. Aplikimi i gjykimit dhe kuptimit të botës reale mund të ndihmojë në pakësimin e këtyre problemeve.

ÇFARË MUND TË BËNI?

Kujtojini fëmijët se veprimet në internet kanë pasoja.

Fjalët që shkruhen nga fëmijët dhe fotot që ato postojnë kanë pasoja në jetën reale.

Fëmijët duhet të publikojnë vetëm gjëra që janë të përshtatshme në pikëpamjen e publikut që i shikon. Pjesë të profilit të fëmijëve tuaj mund të aksesohen nga një audiencë më e gjerë se ju ose persona që njihen prej tyre, edhe nëse përdorin konfigurimet e privatësisë. Inkurajoni fëmijët tuaj që të mendojnë për gjuhën që përdorin në internet dhe t ë mendohen përpara se të postojnë foto dhe video apo të ndryshojnë fotot e publikuara nga dikush tjetër. Punonjësit, zyrtarët e pranimeve në shkolla, trajnerët, mësuesit dhe policia mund t'i shikojë këto publikime.

Kujtojini fëmijët se në momentin që publikuan diçka, nuk mund ta zhbëjnë. Edhe nëse ato fshijnë informacioni nga një faqe, ata kanë shumë pak kontroll mbi publikimet që mund të jenë ruajtur nga pajisje të individëve të tjerë dhe që mund të gjenden në internet. A supozohet që një mesazh të fshihet nga telefoni i një miku? Ka software që lejon ato t'i mbajnë ato.

Duhet t'i thoni fëmijëve të reduktojnë ato që shpërndajnë.

Ndihmoni fëmijët tuaj të kuptojnë se çfarë informacioni duhet të jetë privat. Tregojuni atyre se pse është e rëndësishme që të mbajnë disa gjëra për veten e tyre, familjarët dhe miqtë. Informacion si numri i Sigurisë Shoqërore, adresa, numri i telefonit dhe informacioni financiar i familjes është privat dhe ashtu duhet të qëndrojë.

Flisni me adoleshentët për shmangien e bisedave të nxehta në internet.

Adoleshentët që nuk flasin me të panjohur në internet kanë më pak shanse të bien në kontakt me persona të papërshtatshëm. Në fakt, kërkuesit kanë zbuluar se këta persona zakonisht nuk paraqiten si fëmijë apo adoleshentë dhe shumica e adoleshentëve që kontaktohen nga të rritur që nuk i njohin, bezdisen nga ky fakt. Adoleshentët nuk duhet të hezitojnë që ti bllokojnë apo injorojnë ato dhe t'i besojnë instinktit të tyre kur mendojnë se diçka nuk shkon mirë.

Dërgo me kujdes mesazhet në grup. Sugjerojini fëmijëve tuaj që të mendojnë se kush duhet ta shikojë mesazhin e tyre kur ja dërgojnë disa njerëzve.

Limitoni aksesin në profilet e fëmijëve.

Përdorni konfigurimet e privatësisë. Shumë faqe të rrjeteve sociale, chat-i dhe llogaritë e videove kanë konfigurime privatësie të ndryshueshme, pra ju dhe fëmijët tuaj mund ta limitoni aksesin në profile. Flisni me fëmijët për rëndësinë e këtyre konfigurimeve dhe rreth pritshmërive tuaja se kush duhet të lejohet të shikojë profilin e tyre.

Shqyrtimi i listës së miqve të fëmijës tuaj. Sugjerojini fëmijëve të limitojnë miqtë online për njerëz që i njohin. Pyetini se me kë flasin në internet.

BULLIZMI NË INTERNET

Bullizmi në internet është bullizëm ose ngacmim që ndodh në internet. Kjo mund të ndodhë me anë të një email-i, mesazhi, lojë online apo në një faqe sociale. Mund të përfshijë thashetheme apo foto mbi profilin e dikujt apo të shpërndara që të shihen nga të tjerët.

ÇFARË MUND TË BËSH?

Ndihmoni në parandalimin e bullizmit në internet.

Flisni me fëmijët rreth bullizmit. Tregojini fëmijëve se nuk mund të fshihen nga fjalët që shkruajnë dhe foto që publikojnë apo dërgojnë. Bullizmi është një situatë e humbur: mesazhe të dhimbshme e bëjnë një person të ndihet keq dhe e bëjnë dërguesin të duket keq. Shpeshherë ato mund të tallje nga kolegët dhe dënime nga autoritetet.

Kërkojuni fëmijëve të flasin me ju rreth bullizmit. Kërkojini fëmijëve që t'iu vënë në dijeni kur një mesazh në internet i bën të ndjehen të kërcënuar apo lënduar.

Njihuni me shenjat e bullizmit në internet. Bullizmi në internet shpesh përfshin komente kërcënuese ose fyese. Kontrolloni herë pas here profilin e fëmijës tuaj për të zbuluar ndonjë gjë. A mund të jetë fëmija juaj bullisti? Shikoni për shenja të sjelljes së kësaj natyre si krijimi i imazheve të këqija të një tjetër fëmije.

Ndihmoni në parandalimin e bullizmit.

Mos reagoni ndaj bullistit. Nëse fëmija juaj bëhet objektiv nga një bullizëm në internet, qëndroni gjakftohtë. Kujtojini fëmijës se shumë njerëz e kuptojnë se bullizmi është i gabuar. Thuaju fëmijëve që të mos përgjigjen me përtesë, por inkurajojini ato që të ruajnë provat dhe flasin me ju rreth këtij problemi. Nëse bullizmi vazhdon, ndajeni këtë problem me zyrtarë të shkollës apo me organe ligj-zbatuese.

Mbroni profilin e fëmijës tuaj. Nëse fëmija juaj gjen një profil që është krijuar apo ndryshuar pa lejen e tyre, kontaktoni faqen për të zgjidhur problemin.

Bllokoni ose fshini bullistin. Fshini bullistin nga lista e miqve dhe bllokoni emrin e tyre, adresën e email dhe numrin e telefonit.

PËRDORIMI I PAJISJEVE TELEFON

Cila moshë është më e përshtatshme që një fëmijë të mbajë telefon të zgjuar? Këtë e vendosni ju dhe familja juaj. Konsideroni moshën e fëmijës tuaj, personalitetin, pjekurinë dhe rrethanat e familjes tuaj.

ÇFARË MUND TË BËNI?

Telefonat, karakteristikat dhe opsionet

Vendosni për opsionet dhe karakteristikat e duhura.

Kompania juaj e wireless dhe telefonisë duhet t'iu japë disa zgjedhje për konfigurimet e privatësisë dhe kontrollet e sigurisë së fëmijës. Shumica e bartësve lejon prindërit për të ndaluar karakteristika si aksesi në web, mesazhi apo shkarkimi.

Disa celularë janë bërë posaçërisht për fëmijët. Ato janë projektuar që të jenë lehtësisht në përdorim dhe kanë karakteristika si akses i limituar në internet, menaxhimi i minutës, numri i privatësisë dhe butonat e emergjencës.

Bëhuni të zgjuar me smartphon-at
Shumë telefona ofrojnë akses në internet dhe aplikacione. Nëse fëmijë tuaj do të përdorin një telefon dhe ju jeni të shqetësuar se çfarë mund të gjejnë ato online, zgjidhni një telefon me internet të limituar ose aktivizoni filtrimin në rrjet.

Njihuni me shërbimet e vendndodhjes.
Shumë telefona kanë GPS të instaluar. Fëmijë që kanë këto telefona mund të shikojnë se ku janë miqtë e tyre dhe të lokalizohen nga ato. Kërkojini fëmijëve tuaj që të limitojnë këto opsione që mos të transmetojnë vendndodhjen e tyre. Shpjegojini se mund të ketë mënyra të tjera që t'i lejosh të tjerët të dinë se ku je apo ku janë ato. Si rrjedhojë, disa bartës ofrojnë shërbime GPS që i mundësojnë prindërit të lokalizojnë fëmijët e tyre.

Telefona të mbrojtura me fjalëkalim
Një fjalëkalim, kod numerik, veprim apo shenja e gishtave mund të kyç një telefon nga ndërhyrësit. Kjo nuk parandalon vetëm shtypjen e butonave në xhep pa dashur, por mbron gjithashtu informacione dhe foto që mund të bien në duart e gabuara.

Krijoni rregulla
Shpjegoni se çfarë prisni.
Flisni me fëmijët se kur është koha e përshtatshme për të përdorur telefonat e tyre dhe të të tjerëve. Gjithashtu, ju mundtë doni të vendosni rregulla për përdorim të përgjegjshëm. A i lejoni telefonatat, mesazhet apo lojërat në tavolinën e ngrënies. A keni rregulla për përdorimin e telefonit gjatë natës? A duhet t'iu japin ato telefonat e tyre ndërkohë që bëjnë detyrat apo kur supozohet që të jenë duke fjetur?

Jepni një shembull
Është e paligjshme t'i japësh makinës ndërkohë që dërgon mesazhe apo flet në telefon pa një pajisje hands-free në shumicën e shteteve, por që është e rrezikshme kudo. Vendosni një shembull për fëmijët tuaj dhe flitini atyre për rreziqet dhe pasojat e shpërqendrimit kur i jep makinës.

Rrjetëzimi dhe shpërndarja e informacioneve me telefon.
Socializimi dhe publikimet në internet mund të nxisin krijimtarinë dhe argëtimin por mund të shkaktojë probleme që kanë të bëjnë me reputacionin dhe sigurinë personale.
Tregoni kujdes kur shpërndani foto dhe video.
Shumica e telefonave kanë kamera dhe video si opsion, duke e bërë të lehtë kapjen dhe shpërndarjen e çdo momenti. Inkurajoni që të kërkojnë leje nga fotografi apo personi në foto përpara se të postohen videot apo fotot. Është më e thjeshtë të tregohesh i zgjuar përpara momentit se të kryhet publikimi se sa të kontrollosh dëmin më vonë.

Përdorni gjykimin e duhur me rrjetet sociale nga një pajisje telefoni.
Filtrat që keni instaluar në kompjuterin tuaj në shtëpi nuk do limitojnë fëmijët në veprimet në një telefon. Kërkojini adoleshentëve tuaj për përdorimin e duhur kur janë në rrjete sociale.

Aplikacionet e telefonit
Çfarë duhet të di rreth aplikacioneve?
Aplikacionet mund:
Të mbledhin dhe shpërndajnë informacion personal
Të lejojnë fëmijët tuaj të shpenzojnë para edhe nëse aplikacioni është pa pagesë
Të përfshijë ads
Të lidhen me rrjetet sociale
Por aplikacionet nuk mund t'iu tregojnë se po veprojnë kështu.

ÇARË MUND TË BËSH?

Ja se çfarë mund të bëni ju dhe fëmijët tuaj që të mësoni rreth një aplikacioni përpara se ta shkarkoni atë:
Shikoni fotografimin e ekranit
Lexoni përshkrimin, vlerësimi i përmbajtjes dhe komentet e përdoruesit
Bëni disa kërkime rreth krijuesit, përfshirë komente të jashtme nga burime që janë të besueshme
Kontrolloni se çfarë informacioni mbledh aplikacioni
A mund ta kufizoj përdorimin e aplikacioneve që përdorin fëmijët e mi?
Përpara se t'ia kaloni në duar tabletën apo telefonin fëmijës tuaj, hidhini një sy konfigurimeve. Do të jeni të aftë të:
Kufizoni përmbajtjen se çfarë duhet të shikojë fëmija juaj sipas moshës
Vendosni një fjalëkalim që aplikacionet mos të shkarkohen pa të dhe fëmijët s'mund të blenë asgjë pa të.
C'aktivizoni Wi-Fi-në dhe shërbimet e të dhënave ose vendoseni telefonin në "airplane mode" që mos të lidhet me internetin
Mënyra më e mirë që të vazhduar me aplikacionet e fëmijëve është t'i provoni vetë dhe të flisni me fëmijët tuaj për rregullat e blerjes dhe përdorimit të aplikacioneve.
Shkëmbimi i mesazheve
Inkurajoni mënyrat e mesazhit
Nëse fëmijët tuaj po dërgojnë mesazh, nxitini ato që të respektojnë të tjerët. Mesazhet e shkurtra mund të krijojnë keqkuptime. Tregojuni atyre që të mendojnë se si një mesazh mund të lexohet dhe kuptohet përpara se ta dërgojnë atë.

Ruajtja e privatësisë.
Kujtojini fëmijët që të:
Shmangin mesazhe nga njerëz që nuk i njohin.
Të mësojnë se si të bllokojnë numra nga telefoni i tyre
Shmangja e vënies online të numrit të tyre
Të mos japin kurrë informacion personal apo financiar në përgjigje të një mesazhi
Njihuni me mesazhet spam
Ndihmoni fëmijët tuaj të njohin mesazhet spam dhe shpjegojini pasojat:
Që të zbulojnë informacionin tuaj, shpesh përdoren premtime për dhurata të lira apo ju kërkohet të verifikoni informacionin e llogarisë tuaj
Mund të çojë në shpenzime të padëshiruara në faturë tuaj të telefonit
Mund të ngadalësojë performancën e telefonit

ÇFARË MUND TË BËSH?

Rishikoni faturën tuaj të telefonit për harxhime të paautorizuara dhe raportojini tek bartësi juaj. Tregojuni fëmijëve:
Të fshinë mesazhet që kërkojnë informacion personal
Edhe nëse premtohet ndonjë dhuratë e lirë. Kompanitë e ligjëruara nuk kërkojnë informacion si numrat e llogarisë apo fjalëkalimet me anë të email-it dhe mesazhit.
Mos të përgjigjen apo klikojnë në linket e mesazhit.
Linket mund të instalojnë malware dhe t'iu çojë në faqe false që duken të vërteta por që ekzistojnë vetëm për t'iu vjedhur informacionin.
Sexting
Dërgimi apo përcjellja e fotove, videove apo mesazheve me përmbajtje të nxehta nga një pajisje telefoni njihet me termin "sexting". Kërkojini fëmijëve që mos ta bëjnë këtë. Përveç rrezikut të reputacionit të tyre dhe miqve, ato mund të shkelin edhe ligjin nëse krijojnë, dërgojnë apo ruajnë të tilla mesazhe. Adoleshentët mund të reduktojnë këto sjellje nëse do të dinin pasojat.

Të bësh sigurinë në kompjuter një zakon.

Siguria e kompjuterit, telefonit tuaj, dhe pajisjeve të tjera të telefonit mund të cenojë sigurinë e eksperiencës tuaj online dhe të fëmijëve. Malware mund të lejojë dikë që të vjedhë informacionit personal dhe financiar të familjes tuaj. Malware është software që mund:
Të instalojë viruse
Të monitorojë dhe kontrollojë përdorimin e kompjuterit tuaj
Të dërgojë pop-up ads të padëshiruara
Të lidhë pajisjen tuaj me faqe që nuk po i kërkoni
Të regjistrojë përdorimin e tastierës.

ÇFARË MUND TË BËSH?

Përdorni sigurinë software dhe mbajeni të përditësuar

Kompanitë e mirënjohura ofrojnë shumë opsione të lira. Vendoseni software që të përditësohet automatikisht.

Mbani sistemin operativ dhe rrjetin browser të përditësuar. Kamerat shfrytëzojnë avantazhin e software që nuk ka përditësimet e fundit të sigurisë. Gjithashtu mund të ndryshoni sigurinë dhe konfigurimet e privatësisë në sistemin operativ apo browser. Kontrollo mjetet ose opsionet për të eksploruar zgjedhjet tuaja. Kur jeni në të, përditësoni dhe aplikacionet tuaja gjithashtu.

Mësojini fëmijëve sigurinë e kompjuterit

Flisni me fëmijët për mënyrën se si ato mund të ndihmojnë të mbrojnë pajisjet e tyre dhe informacionin personal të familjes tuaj.

Krijoni fjalëkalime të sigurt dhe mbajini privat.

Sa më i gjatë të jetë fjalëkalimi, aq më e vështirë është të deshifrohet. Data e lindjes, emri i log-imit, apo fjalë të përbashkëta nuk janë fjalëkalime të sigurt. Kërkojini fëmijëve të jenë krijues dhe të kenë fjalëkalime të ndryshme për çdo llogari.

Mund të jetë tunduese për të përdorur të njëjtin fjalëkalim, por nëse vidhet, hakerat mund ta përdorin për të aksesuar llogari të tjera. Fëmijët mund të mbrojnë gjithashtu fjalëkalimet e tyre duke mos i ndarë me askënd tjetër, përfshirë këtu miqtë e tyre.

Mos jepni informacion personal dhe financiar nëse faqja nuk është e sigurt.

Nëse ju dhe fëmijët tuaj dërgoni mesazhe, shpërndani foto, përdorni rrjete sociale, apo kryeni veprime bankare online, po dërgoni informacion personal në internet. Mësojini fëmijët: nëse URL nuk fillon me https, mos vendosni asnjë informacion personal. Ajo "s" qëndron për siguri. Kjo do të thotë se informacioni që po dërgoni është i enkriptuar dhe i mbrojtur.

Kini kujdes për "free stuff".

Lojërat, aplikacionet, muzika dhe materiale të tjera që janë të lira mund të fshehin malware. Mos shkarkoni gjë nëse nuk i besoni burimit. Mësojini fëmijët se si të njohin burime të sigurta.

Jini të kujdesshëm për P2P file-sharing.

Disa fëmijë shpërndajnë muzikë, lojëra apo softëare online. Shkëmbimi i informacioneve P2P mundëson njerëzit në ndarjen e këtyre informacioneve nëpërmjet një rrjeti jo formal kompjuterësh që punojnë me të njëjtin software.

Ndonjëherë, spyware, malware apo pornografia mund të fshihet në një dosje. Nëse fëmijët tuaj shkarkojnë një material me të drejtë autori, mund të jeni subjekt për shkelje të ligjit. Është e rëndësishme që t'i flisni fëmijëve tuaj për sigurinë dhe rreziqeve të tjera të përfshira me shpërndarjen e informacioneve. Instaloni software e shpërndarjes së informacioneve siç duhet. Kontrolloni default settings që mos të ndahet asgjë që është private. Me parazgjedhje, thuajse të gjitha aplikacionet P2P të shpërndarjes së informacioneve do të shpërndajë të dhëna në dosjet "Downloads" ose "Shared".

Nëse ruani dosje personale në folder të shpërndarë, përdorues të tjerë të P2P mund të aksesojë dosje që nuk doni t'i ndani – përfshirë dokumente private si pagesat e taksave apo dokumente të tjera financiare. Përdorni software të sigurisë për të skanuar informacione. Përpara se fëmija juaj të hapë apo luajë ndonjë material të shkarkuar, përdor software të sigurisë për ta skanuar. Sigurohuni që software i sigurisë të jetë i përditësuar dhe funksional.

Përdorimi i sigurt i Wi-Fi publike

Shumë vende publike si kafenetë, libraritë dhe aeroportet ofrojnë internet Wi-Fi. Interneti mund të jetë i përshtatshëm, por shpesh nuk janë të sigurt. Kjo gjë do të lehtësonte punën e dikujt për të aksesuar llogaritë online të familjes tuaj apo të vjedhë informacionin tuaj personal, përfshirë dokumentet private, fotot dhe fjalëkalimet.

CFARË MUND TË BËSH?

Përdor rrjete të sigurta Wi-Fi.

Rrjetet e sigurta përdorin enkriptimin, i cili mbron informacionin që dërgon online duke e fshehur atë në mënyrë që të tjerët mos të kenë akses mbi të. Mund të jeni të sigurt se një rrjet është i sigurt vetëm nëse të kërkohet të japësh një fjalëkalim WPA apo WPA2.

Tregojuni fëmijëve se nëse nuk iu kërkohet fjalëkalimi, nuk duhet të nënshkruhen në asnjë llogari apo të dërgojnë informacion personal. Mos mendoni se Wi-Fi hotspot përdor enkriptim: shumica e tyre nuk e bëjnë.

Përdorni website të sigurta.

Një faqe e sigurt do të enkriptojë informacionin tuaj ndërkohë që jeni nënshkruar në të edhe nëse rrjeti nuk e bën. Si do ta dinë fëmijët tuaj se si një faqe është e sigurt? Tregojuni atyre që të shikojnë për https në adresat e rrjetit të çdo faqeje që vizitojnë, jo vetëm kur log-ohen. "s" qëndron për siguri.

Mos qëndroni përgjithmonë të nënshkruar nëpër llogari.

Rekomandojini fëmijëve që të dalin nga llogaria pasi të kenë mbaruar.

Phishing Scams (mënyrë për të vjedhur informacione)

Phishing ndodh kur një person dërgon mesazhe, email-e apo mesazhe pop-up për të tërhequr njerëz në mënyrë që të shpërndajnë informacioni e tyre personal dhe financiar. Scammers-at e përdorin këtë informacion për të aksesuar llogaritë tuaja, të vjedhin identitetin dhe të kryejë mashtrime.

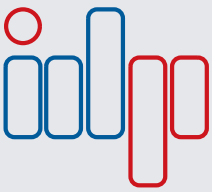
ÇFARË MUND TË BËSH?

Ja se si ju dhe fëmijët tuaj mund të shmangni mashtrimet nga një artist scam.

Mos u përgjigjeni mesazheve, email-eve, apo mesazheve pop-up që kërkojnë informacion personal apo financiar dhe mos klikoni asnjë link në mesazh.

Jini të kujdesshëm kur hapni ndonjë dokument bashkëlidhur apo të shkarkoni ndonjë dosje nga email-et që ju vijnë, pavarësisht se kushi dërgon. Materiale të papritura mund të përmbajnë viruse që nuk dihen nga miqtë dhe familjarët tuaj.

Përfshini fëmijët tuaj, që ato të zhvillojnë "antenat scam" dhe të kenë kujdes në internet. Shikoni për momente që ju mësojnë, nëse merrni një mesazh phishing, tregojuani fëmijëve tuaj që të kuptojnë se gjërat nuk janë gjithmonë ashtu siç duken.



KOMISIONERI PËR TË DREJTËN
E INFORMIMIT DHE MBROJTJEN
E TË DHËNAVE PERSONALE

Adresa: Rr. "Abdi Toptani", Nd. 5,
Kodi postar 1001, Tiranë
E-mail: info@idp.al
TEL: +35542237200
FAX: +35542233977
Nr. i Gjelbër: 08002050

www.idp.al