KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJENE TË DHËNAVE PERSONALE

KUJDES NGA VJEDHJA E IDENTITETIT TUAJ !

PORTOFOLI JUAJ

Portofoli juaj mban shumë informacion në lidhje me ju. Ky informacion mund të keqpërdoret.

Dokumentet e identitetit të tilla si karta e identitetit dhe patenta e shoferit janë veçanërisht tërheqëse për hajdutët e identitetit. Kjo për shkak se një hajdut i identitetit mund të përdorë këto si identitet të rremë, ose si një burim për të gjetur më shumë informacion rreth jush.

Gjithmonë sigurohuni të dini se ku janë të ruajtura dokumentet tuaja të identitetit. Ju duhet të kini kujdes dhe të siguroheni që dokumentet janë të ruajtura në një vend të sigurt. Dokumentet që ju i përdorni rrallë mund të vendosen në një kuti të depozitave të sigurisë. Ju duhet të bëni një sistemim të rregullt të portofolit tuaj, hiqni kartat dhe dokumentet e tjera që ju nuk keni nevojë që të jenë në portofolin tuaj.

Nëse një dokument identiteti është vjedhur apo humbur, njoftoni menjëherë policinë dhe autoritetet e tjera përkatëse.

Mbani numrat e kontaktit të bankës tuaj apo të agjencive të tjera ku ju mund të telefononi për çdo rast që keni nevojë për të bllokuar një kartë debiti ose krediti.

KUTIA JUAJ POSTARE

Informacione personale nga më të ndryshmet mund të dërgohen me postë në kutinë tuaj postare, duke përfshirë fatura të ndryshme, kartat e kreditit apo debiti, formate dhe dokumente te tjera. Kjo zakonisht nuk është diçka që ju mund të shmangni. Megjithatë, ju mund të bëni diçka për të zvogëluar rreziqet që informacioni i dërguar me postë të mos mund të vidhet dhe të keqpërdoret.

Vendosni një çelës në kutinë tuaj postare. Nëse ju jeni në pushime lajmëroni një fqinj për të mbledhur postën tuaj, ose kërkoni në zyrën postare ndalimin e dërgimit të letrave në kutinë tuaj postare gjatë kohës që ju jeni larg shtëpisë. Në këtë mënyrë kutia Juaj postare nuk do të mbushet dhe nuk do të ketë rrezik që letrat të ndodhura në kuti të devijojnë jashtë saj.

KOSHI JUAJ I MBETURINAVE

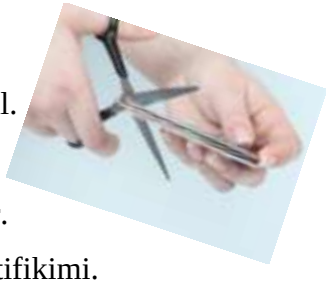
Besojini apo jo, hajdutët e identitetit shkojnë në kazanët e mbeturinave dhe dokumentet që janë pa interes për ju mund të jetë një minierë floriri informacioni për një kriminel.

Kjo është për shkak se ato dokumente mund të përfshijnë informacion rreth jush dhe një hajdut identiteti mund të përdorë.

Për shembull, dokumenti që mund të mbajë lidhjet me kontaktet tuaja, njerëzit që ju njihni- hajduti mund të lidhet me ta dhe pretendojë të jetë ju. Bizneset mund të mashtrohen lehtë në qoftë se një hajdut identiteti mund të japë informacion që vetëm ju duhet ta dini.

Dokumentet gjithashtu mund të përfshijnë detaje që një hajdut identiteti i ka të nevojshme për të ndërtuar një profil sikur të jeni ju.

Grisini të gjitha dokumentet që përmbajnë informacion në lidhje me ju para se të hidhni ato në një kazan mbeturinash. Ju mund të merrni makina grirëse të cilat quhen “shredding”. Për shëmbull dokumentet që duhet gjithmonë të shkatërrohen përpara se ti hidhni janë :



- Karta e kreditit ose debiti si dhe faturat.
- Aplikacionet personale.
- Disqe CD apo DVD me informacion personal.
- Dokumente pagesash.
- Dokumentet e regjistrimit që ju kanë skaduar.
- Dokumente të përmbajnë ndonjë numër identifikimi.
- Copëtoni kartat e pavlefshme ose të skaduara të identitetit para se ti hedhni ato, për t'u siguruar që ata nuk mund të përdoret më pas.
- Smash disqet përmbajnë informacion personal dixhital.
- Dokumente si certifikata e lindjes, diplomave, certifikata e martesës dhe certifikatat e sigurimit.

KOMPJUTERI JUAJ PERSONAL

Ju përdorni kompjuterët tuaj për të ruajtur shumë informacion në lidhje me jetën tuaj dhe për çfarë ju jeni të interesuar, të tilla si dokumente tuaj personale, fotografi, filma, muzikë e të tjera.

Kompjuteri juaj gjithashtu lidhet me internetin, me rrjete ku ju jeni veçanërisht të prekshëm për vjedhjet e identitetit. Pra, është e rëndësishme për të mbrojtur kompjuterin tuaj kundër ndërhyrjes së mundshme, për të parandaluar qasje në të gjitha në informacionet të cilat ndodhen në kompjuterin personal.

Disa këshilla :

- Kurrë mos e lini laptopin në makinë ose në vende të tjera ku kjo është e dukshme dhe joshëse për hajdutët.
- Përdorni një "fireëall" personal. (Kjo është zakonisht një mbrojtëse softuer).
- Përdorni anti-virus software dhe përditësoni atë në datën që skadon.
- Gjithmonë përdorni kontrolle automatike për përditësime, kontrolloni nëse përditësimet e sigurisë për aplikacionet tuaja janë instaluar.
- Ç'instaloni programe që ju nuk i përdorni.
- Sigurohuni që të gjitha informacionet tuaja personale janë fshirë nga kompjuteri juaj para se ta shisni atë. Vetëm duke shtypur butonin 'delete' nuk është e mjaftueshme, hiqini dhe shkatërrojini nga hard drive ose përdorni opsionin e formatimit për të siguruar që asnjë informacion personal nuk mund të shikohet.

BLERJA ONLINE.

Blerjet në internet mund të jetë shumë efektive dhe të leverdishme, por gjithashtu nga ana tjetër mund të rrisin rrezikun për vjedhje.

Nëse jeni të pasigurt në lidhje me një faqe interneti, mos e përdorni atë. Kontrolloni nëse adresa në të cilin dëshironi të bëni blerjen është një biznes legjitim. Jo të gjitha faqet e internetit janë ata që duken të jenë, dhe ju duhet të keni kujdes mos të keni ndërhyrës që mund të monitorojnë transaksionet tuaja.

Disa këshilla :

- Nëse ju jeni duke paguar diçka online, sigurohuni që seksioni i internetit është koduar (adresa fillon me "https"). Ju gjithashtu duhet të shikoni për 'dry' në shiritin e adresave.
- Para se të bëni blerje online në një adresë që ju nuk e keni përdorur më parë duhet të:
  - Testoni – 'links'.
  - Telefononi shërbimin e konsumatorit që të jeni të sigurt që biznesi ekziston në të vërtetë.
  - Bëni pyetje shërbimit të klientit në lidhje me biznesin.
- Gjithmonë sigurohuni që ju të merrni një vërtetim ose konfirmim të blerjes kur bëni pazar me interes. Çdo biznes legjitim duhet t'ju dërgoj një të tillë.
- Gjithmonë mbani mend që të dilni *'log out'* nga shërbimet bankare të internetit dhe të portaleve publike kur keni bërë blerjet në internet. Kjo mund të parandalojë hakerat që duan të marrin informacion rreth jush.

- Kurrë mos jepni passëordin (fjalëkalimin) ose pin-in(kodin e sigurisë) me telefon apo e-mail.
- Asnjëherë mos ju përgjigjuni ose klikoni në e-maile që kërkojnë të dhënat tuaj personale. Janë ndoshta hajdutë të cilët janë duke u përpjekur për të marrë informacion rreth jush.

TELEFONI JUAJ CELULAR

Ju duhet të siguroni telefonin tuaj celular. Telefonat e fundit celularë janë në të vërtetë kompjuter të vegjël me funksionalitet në rritje.

Telefoni celular mund të mbajë të gjitha llojet e informacionit në lidhje me punën tuaj dhe aktivitetet tuaja private. Pra, një telefon celular është një mjet shumë i vlefshëm për një hajdut identiteti.

Kushdo që mund të marrë telefonin tuaj mund të fitojë qasje në kontaktet tuaja dhe të marrë informacion për ju dhe çfarë ju bëni.

Disa këshilla.

Mos ruani të dhëna sensitivë në telefonin tuaj celular. Ju duhet të shmangin veçanërisht ruajtjen e :

- informacionit bankar që ju vjen me internet, bilanci i bankës dhe numrin e kartës.
- emaile private apo emaile që kanë lidhje me punën tuaj.
- fjalëkalimet dhe kodet e sigurisë (pin).

Rriteni sigurinë në telefonin tuaj dukë :

- përdorur një PIN ose një fjalëkalim.
- kriptuar telefonin, nëse kjo është e disponueshme.
- kontaktuar kompaninë tuaj të telefonit dhe të bllokoni numrin tuaj në qoftë se telefoni juaj ka humbur ose është vjedhur.
- kontrolluar faturat e telefonit tuaj. Sigurohuni që edhe shumat më të vogla janë të sakta. Hajdutët e identitetit shpesh fillojnë me sasi të vogla, për të kontrolluar nëse ju jeni të vëmendshëm. Nëse ju mendoni se diçka që nuk funksionon, hetoni menjëherë.

FJALËKALIMET APO KODET

Mendo për kodet tuaja të sigurisë, ruajini pinet dhe fjalëkalimet në të njëjtën mënyrë si çelësat e shtëpisë. Sikurse ju mbani çelësat tuaj të sigurt, të njëjtën gjë duhet të bëni me fjalëkalimet dhe kodet tuaja.

Nëse dikush merr fjalëkalimet tuaja, ai e ka të lehtë të shtiret si ju, ai gjithashtu mund të ndryshojë ose të krijojë llogari apo network-social në emrin tuaj.

Nëse një hajdut identiteti merr qasje në llogarinë tuaj social-networking, ai gjithashtu do të marr qasje në kontaktet tuaja.

Pyesni bankën tuaj nëse ju mund të vendosni një PIN apo fjalëkalimin që ju mund ta përdorni për të provuar identitetin

tuaj, kjo do të ju ndihmojë për të mbrojtur informacionin tuaj bankar nga hajdutët.

Disa këshilla.

- Përdor një fjalëkalim që është e lehtë për t'u kujtuar, por nga ana tjetër unik dhe i vështirë për t'u identifikuar. Për shembull mos përdorni emrin tuaj ose të anëtarëve të familjes pasi dikush që është i interesuar do ta kishte të lehtë për të identifikuar fjalëkalimin tuaj.
- Përdorni fjalëkalime të ndryshme për çdo shërbim apo llogari, për shembull fjalëkalime të ndryshme për e-mail, për shërbimin bankar apo rrjete sociale.
- Nëse ju keni nevojë t'i shkruani fjalëkalimet tuaja apo kodet, ruani ato në një vend të sigurt të veçantë, që vetëm ju e dini. Nëse ju mund të mësoni përmendësh ato, bëjini - dhe grisni ose digjni fletën ku i keni shkruar.
- Kurrë mos i jepni PIN-in tuaj ose fjalëkalimin dikujt që pretendon që do të ju ndihmojë, siç mund të jetë punonjësit e bankave, shërbimi ndaj klientit apo të tjerëve - qoftë personalisht, në telefon ose online.
- Sigurohuni që askush nuk shikon mbi supe tuaj, kur ju jeni duke shtypur PIN-in tuaj në një automat.
- Mbuloni dorën tuaj ndërkohë që shkruani numrin e kodit në mënyrë që çdo aparat i fshehur të mos mund shikojë numrin tuaj.
- Mendoni kur përdorni kartat e pagesës, sidomos kur ndodheni jashtë vendit. Vlerësoni se sa i sigurt është përdorimi i kartës. Nëse jeni në dyshim, përdorni të hollat.

NUMRI I SIGURIMEVE SHOQËRORE

Një numër i sigurimeve shoqërore është një identifikues shtetëror i autorizuar, i përhershëm dhe unik. Ky numër ju ndjek ju nga lindja deri në vdekje. Ju gjithashtu e përdorni atë në shumë situata për të vetëtuar se kush ju jeni. Prandaj numri i sigurimeve shoqërore është një mjet jashtëzakonisht i rëndësishëm për një hajdut identitetit.

Hajduti i identiteti për shembull mund të mbledhë informacion rreth jush nga burime të ndryshme duke përdorur këtë numër me agjencitë publike ose me kompani të ndryshme që ju keni marrëdhënie. Një hajdut identiteti mund të pretendojë të jetë ju, dhe mund të marrë kredi ose të marrë përfitime të tjera në emrin tuaj.

Disa këshilla.

- Të jeni shumë të kujdesshëm në lidhje me shpërndarjen apo dhënien e numrin tuaj të sigurimit. Duhet të vlerësoni a duhet patjetër ta jepni atë? Nëse jeni të pasigurt, gjithmonë të kërkoni pse është e nevojshme dhënia e numrin tuaj të sigurimit. Agjencitë publike, punëdhënësit dhe institucionet financiare mund të kenë nevojë për numrin tuaj të sigurimit, por ata duhet të jenë në gjendje të shpjegojnë përse kjo është e nevojshme.
- Asnjëherë mos i dërgoni dikujt numrin tuaj të sigurimit me anë një linjë të pasigurt ose me faks. Nëse ju nuk duhet ta dërgoni atë, përdorni përherë një e-mail të kriptuar.
- Merrni masa të menjëhershme nëse ju gjeni numrin tuaj të sigurimit në një dokumentet ku nuk duhet të jetë.

Kontaktoni me ata që ju kanë dërguar këtë dokument dhe kërkoni përse ata e kanë numrin tuaj të sigurimeve shoqërore dhe pse ata duhet të përdorin atë.

- Zgjidhni bizneset që nuk e përdorin numrin e sigurimeve shoqërore, si një pjesë identifikuese e konsumatorëve, ose si një pjesë e kredencialeve të identifikimit.

KARTAT E DEBITIT DHE KREDITIT

Ne përdorim kartat e kreditit dhe debitit gjatë gjithë kohës, por ne duhet të jemi të kujdesshëm. Kurrë mos i jepni të dhënat e kartës së kreditit me anë të telefonit apo internetit, pa qenë absolutisht i sigurt për personin që ju jeni duke komunikuar me të.

Hajdutët e identitetit janë veçanërisht të interesuar për numrin e kartës tuaj, datët e skadimit dhe kodin e sigurisë në anën e pasme të kartës. Kurrë mos lini larg syve tuaj kartat tuaja të kreditit ose debit.

Disa këshilla.

- Gjithmonë kontrolloni detajet e llogarisë tuaj dhe faturat. Merrni masa të menjëhershme në qoftë se edhe shuma të vogla apo të parëndësishme janë të pasakta. Kjo mund të jetë fillimi i një përpjekje në vjedhjen e identitetit tuaj. Njoftoni kompaninë e kartës tuaj në qoftë se diçka duket jo e rregullt, edhe nëse ju thjesht i ndjeheni i pa sigurtë.
- Krijo një listë të numrave të kartave, datën e skadimit dhe detajet e kontaktit për kompaninë e kartës dhe ruani këtë listë në një vend të sigurt. Kjo mund të jetë e dobishme në qoftë se një kartë e juaj është humbur ose vjedhur dhe keni nevojë për të marrë në telefon për ta bllokuar atë.
- Mbani në vëmendje datën e skadimit të kartës tuaj. Nëse ju nuk merrni një kartë zëvendësimi brenda një kohe të arsyeshme para datës së skadimit, kontaktoni kompaninë e kartës menjëherë. Një hajdut identiteti mund të ketë vjedhur kartën e zëvendësimit nga kutia juaj postare. Nëse ju dyshoni që karta juaj është vjedhur, bllokoni menjëherë llogarinë tuaj.
- Gjithmonë bllokoni menjëherë llogarinë që ka qenë e ekspozuar ndaj tërheqjeve të paautorizuar. Pyetni për konfirmim me shkrim që llogaria është mbyllur. Prisni ose copëtoni kartat para se ti hidhni ato. Karta juaj mund të ketë gjithashtu të dhënat të identifikimit tuaj në pjesën e pasme që mund të përdoret si një kartë ID, kështu që gjithmonë të kujdeseni se ku ndodhen kartat tuaja dhe t'i mbani ato të sigurta.
- Mos lini kartën larg syve tuaj në një bar apo restorant. Shikoni se çfarë bën kamerieri me atë - ruhuni nga 'double-sëiping' që mund të tregojë që karta juaj mund të jetë klonuar.

SHPËRNDARJA E INFORMACIONIT PERSONAL

Telefoni është një mjet shumë i dobishëm për hajdutët e identitetit. Nëse ju nuk jeni të kujdesshëm, mund të jetë mjaft e lehtë për hajdutët për të mbledhur informacion nga ju apo kontaktet tuaja dhe pastaj ta përdori këtë informacion kundër jush.

Individët vendosin shumë informacion në lidhje me veten online, sidomos në faqet e rrjeteve sociale. Hakerët ose hajdutët e identitetit mund të jenë në gjendje për të hyrë në llogaritë e përdoruesve. Viruset gjithashtu mund të mbledhin dhe të shpërndajë informacion nga kompjuteri juaj.

Disa këshilla:

- Mos jepni informacion në faqet e rrjeteve sociale që nuk janë të gatshëm për të siguruar atë. Njihuni me parametrat e sigurisë në faqen sociale të internetit (p.sh. Facebook ose Tëitter) dhe ndryshoni fjalëkalimet shpesh, përdorni fjalëkalime të ndryshme për çdo faqe apo adresë që vizitoni.
- Kurrë mos iu përgjigjni ose mos klikoni kërkesat për informacion personal në email. Kërkesa mund të jetë nga një hajdut i cili është duke u përpjekur për të marrë informacion nga ju.

Nëse dëshironi të merrni informacion rreth **Komisionerit për Mbrojtjen e të Dhënave Personale,** Ju lutemi kontaktoni si më poshtë:

Adresa: Rr. e Kavajës, Nd 80, H.1, Tiranë T

Telefoni: +35542237200

e-maili: info@idp.al

Website: www.idp.al