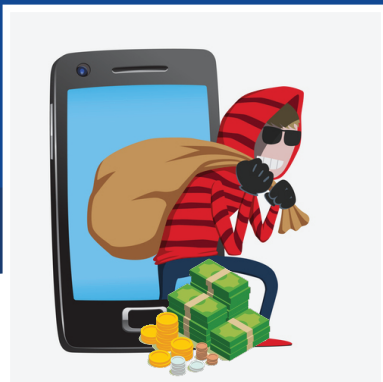




Dukuria e krimeve kibernetike që në vete ngërthen disa vepra penale, është në rritje enorme dhe prekë të gjitha kategoritë e shoqërisë andaj edhe është shqetësuese.

Nga hetimi i veprave penale të krimeve kibernetike, rezulton se ka shumë raste që nuk janë raportuar dhe se shumë persona që janë atakuar sidomos të gjinisë femërore që u janë hakuar llogaritë dhe janë të shantazhuara, kanë hezitur ti raportojnë këto raste në polici.

Si pasojë e mos-raportimit, pakujdesisë apo mos njohurisë së përdorimit të internetit, ka shembuj të rasteve reale që kanë ndodhur kohët e fundit dhe rastet e tilla kanë tendencë të rritjes gjithnjë e më shumë. Disa nga shembujt real:

- Disa persona janë vënë në lajthitje dhe kanë dërguar të holla në shtete të ndryshme, ku keqpërdoruesit/mashtguesit krijojnë llogari të rrejshme dhe paraqiten se janë punonjës banke, avokatë apo profesione kredibile të tjera duke ju shkruar- dërguar viktimave mesazhe nga rrjetet sociale apo e-mail se një person që ka vdekur ka qenë familjar i viktimave gjoja se ai ka lënë trashëgimi shuma të mëdha parash edhe i rekomandojnë viktimat që të aplikojnë për të trashëguar të hollat. Më pas ata viktimën e vënë në lajthitje se duhet të kryejnë disa pagesa për të përfunduar procedurat e nevojshme të dokumentacionit të trashëgimit të pasurisë dhe se viktimat paguajnë shuma të ndryshme tek persona që nuk iu dihet as origjina e shtetit se nga vijnë.

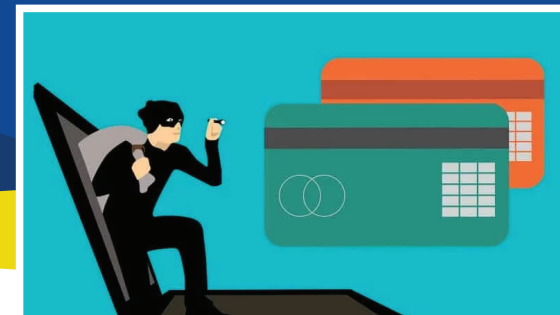


- Personat që janë vënë në lajthitje dhe kanë dërguar të holla në shtete të ndryshme, ku keqpërdoruesit/mashtguesit krijojnë llogari të rrejshme dhe paraqiten se janë persona bamirës dhe viktimës i shënojnë mesazh nga rrjetet sociale apo përmes e-mail, se janë të interesuar të hapin spitale në Kosovë. Më pas ata viktimën e vënë në lajthitje se duhet të kryejnë disa pagesa për të përfunduar procedurat e nevojshme të dokumentacionit për të marrë përqindje nga investimi.

- Në disa raste keqpërdoruesit/mashtguesit krijojnë llogari të rrejshme dhe paraqiten se janë femra dhe gjatë komunikimit kërkojnë nga viktimat foto të ndryshme. Më pas të dyshuarit e shantazhojnë viktimën duke i përdorur fotot që për ti mos i publikuar, viktimat ti dërgojnë shumen e caktuar të parave në institucione mikrofinanciare.

- Raste tjera janë evidentuar ku viktimave ju vijnë mesazhe me një link të infektuar me virus, mesazhi mund të vijë nga persona të njohur apo të panjohur si dhe mesazhi me përmbajtje se fotografitë tuaja janë shpërndarë nëpër internet dhe për ti larguar fotografitë i kërkohet që të dërgojnë fotografi të tjera për ti fshirë nga interneti fotot të cilat kinse janë shpërndarë, në këto raste pjesa dërmuese e viktimave i përkasin gjenisë femërore.

- Kohëve te fundit është shprehur edhe dukuria e mashtimit ku i dyshuari e hakon llogarinë e viktimës dhe me pas nga ajo llogari i shkruan shokëve dhe shoqeve te viktimës, ku u kërkon të holla në emër te tij se gjoja ai është dhe i shtrirë ne spital jashtë vendi i dhe se për shërim i nevojiten shuma të caktuara të parave dhe kërkon që këto para ti dërgohen përmes institucioneve financiare jo-bankare apo zyra të transferimit të parave..



- Gjithashtu kohët e fundit ka edhe raportime të rasteve kur nga llogarite bankare të viktimës në bankat e Kosovës ka pasur blerje apo tërheqje online pa autorizimin e tij/saj. Në të gjitha këto raste keqpërdoruesit gjatë komunikimit përdorin ose shfrytëzojnë aplikacionin online "Google translate" mesazhet ju dërgohen viktimave në gjuhën shqipe.

Rezultatet nga keqpërdorimet kibernetike

- ✓ Kujdes, llogaria juaj mund të ju keqpërdoret (hakohet)!
- ✓ Disa nga linçet (të rrejshme) krijohen për të keqpërdorur/mashtuar llogarinë tuaj!
- ✓ Mos hapni, mos aplikoni në secilin aplikacion që nuk e dini prejardhjen (vërtetësinë e tij)
- ✓ Kujdes gjatë blerjeve online me kartela bankare në web faqe të panjohura!

Masat e sigurisë

- ✓ Para se të japësh të dhënat tuaja personale sigurohu për besueshmërinë e adresës-linkut!
- ✓ Mos shkarkoni aplikacione dhe webfaqe të pasigurta!
- ✓ Aplikimi me të dhënat tuja në linqe të ndryshme lehtësisht mund të keqpërdoret!
- ✓ Mos jepni numra personal te dokumenteve tuaja te identifikimit!
- ✓ Mos jepni numrat e xhirollogarisë suaj bankare dhe tre numrat e (kodin e sigurisë) te kartelës suaj te cilët janë te vendosur ne anën e mbrapsme te kartelës bankare!

Mos jepni te dhëna tjera personale



Kujdes:

- ✓ Dukurinë e keqpërdorimit të krimeve kibernetike mund ta hasim kudo.
- ✓ Zhvillimi dhe avancimi i teknologjisë përveç se i domosdoshëm bart me vete edhe rreziqet e mundshme!

Për çdo dyshim të keqpërdorimit apo shantazhit RAPORTONI në Polici në linjën **192**, aplikacionin mobil "Lajmëro Policinë" ose e-mail info@kosovopolic.com

DRP Mitrovicë Jugu



VETËDIJESIMI PËR RREZIQET NGA KEQPERDORIMET DHE KRIMET KIBERNETIKE

