САЈБЕР БЕЗБЕДНОСТ: ПРАКТИЧНИ СОВЕТИ ЗА ГРАЃАНИТЕ КАКО ДА СЕ ЗАШТИТАТ ОД ИЗМАМИ НА ИНТЕРНЕТ

ШТО Е ИЗМАМА НА ИНТЕРНЕТ?

Терминот измама на интернет општо се однесува на активности на компјутерски криминал што се одвива преку интернет (е-пошта, социјални мрежи, онлајн услуги), вклучувајќи кривични дела како кражба на идентитет, „фишинг“и други хакерски и измамнички активности со цел да се измамат луѓе, за да се украдат нивните лични податоци и пари.

НАЈЧЕСТИ ИЗМАМИ НА ИНТЕРНЕТ И ЗЛОУПОТРЕБА НА ВАШИТЕ ЛИЧНИ ПОДАТОЦИ

1) ЗЛОНАМЕРЕН СОФТВЕР (СОФТВЕР ЗА УЦЕНИ И ОТКУП)

Пример: Добивате е-пошта: „На вашиот компјутер инсталиравме злонамерна компјутерска програма (злонамерен софтвер) преку која добивме пристап до вашите лични податоци. Платете 1500 евра во биткоини доколку не сакате јавно да ги откриеме вашите лични податоци.“

Уценувачот наведува дека поседува снимка од веб камерата на вашиот компјутер до која пристапил додека вие наводно сте гледале веб страници со порнографска содржина. Притоа, тој се заканува дека ќе им објави наводно „понижувачко“ видео на сите ваши контакти што ги собрал од Фејсбук и од вашата е-пошта.

Друг вообичаен пример за измама на интернет е откупувачкиот софтвер (ransomware).

Пример: Добивате е-пошта од непозната адреса во која испраќачот тврди дека сте нарачале стока/услуга и дека треба да извршите плаќање. Е-поштата исто така содржи прилог со упатства за плаќање.

Откако ќе го отворите прилогот што го добивте во е-поштата, уценувачот ја презема контролата над вашиот компјутер и ги криптира сите датотеки и без да го знаете конкретниот клуч повеќе не можете да пристапите до вашите лични податоци. Уценувачот бара од вас да го платите откупот, а за возврат ќе го добиете клучот за декриптирање на вашите податоци.

БИДЕТЕ ВНИМАТЕЛНИ: Не одговарајте на вакви пораки и не давајте им пари на уценувачите. Доколку сте отвориле прилог кој содржи злонамерен код, известете ја полицијата! Променете ја лозинката за пристап до вашата е-пошта! Не ги внесувајте вашите кориснички податоци, лозинки и други лични информации на сомнителни веб страници!

Овој проект е финансиран од Европската Унија

На линкот „Have I Been Pwned“ https://haveibeenpwned.com/, проверете ги СИТЕ ваши електронски адреси (е-пошти) што ги користите, на овој начин можете да проверите дали се компромитирани или се во хакерски бази на податоци.

Доколку дадената адреса за е-пошта е компромитирана, ве советуваме да го направите следново:

- Од претпазливост променете ја лозинката за оваа електронска адреса со нова силна безбедносна лозинка.
- Во сите интернет услуги и услуги каде што сте ја користеле оваа електронска адреса за да се најавите (на пр. социјални мрежи, е-продавница итн.) креирајте нова силна безбедносна лозинка за секоја од овие услуги. Ако услугата на интернет или другата услуга ја нуди опцијата за двофакторска автентикација (two factor authentication), би било препорачливо да се вклучи оваа опција.

Користете силна и уникатна лозинка за секоја од вашите сметки на социјалните мрежи за да го спречите нивното евентуално хакирање.

Одбегнувајте очигледни лозинки како што се моминското презиме на мајката, името на детето, датумот на раѓање, општи лозинки или што било друго што некој може да го погоди преку информациите што сте ги објавиле за себе.

Силната лозинка треба да содржи:

- 16 **или повеќе карактери**,
- **Големи букви** (ABCDEFGH...),
- **Мали букви** (abcdefgh...),
- **Бројки** (123456...),
- **Симболи** (@#$%{ } [ ] ( ) / \ ‘ ” , ; : . < >...)

2) „ФИШИНГ“

„Фишингот“ се однесува на онлајн измамничка е-пошта или пораки испратени преку социјалните мрежи кои се чини дека се испратени од легитимни организации (како банка или е-продавница) што го наведуваат примачот да споделува лични, финансиски или безбедносни информации. На овој начин измамниците добиваат пристап до кориснички имиња, лозинки или податоци од кредитни картички. Во таквата е-пошта најчесто се бара да го преземете приложениот документ или да кликнете на врската.

Пример: Измамник сака да купи производ од жртва. Тој ги наоѓа своите жртви преку е-продавница каде што луѓето ги продаваат своите предмети што веќе не ги користат (автомобили, облека, чевли, мебел, домашни апарати, книги итн.). Тој испраќа порака до својата жртва во која тврди дека сака да купи фрижидер од неа. Измамникот ѝ вели на својата жртва дека треба да ја плати поштарината и потоа ѝ испраќа линк до веб страница на компанија за услуги за испорака. Во одреден момент го испраќа и копчето „Потврди“ и откако жртвата ќе кликне на него, се отвора линк од веб страница на банка и од жртвата се бара да ги даде своите финансиски податоци. Ова се „фишинг“ (phishing) страници кои изгледаат како веб страници за услуга за испорака и на банка. Целта е да се украдат личните податоци на жртвата и да се злоупотребат за пари.

БИДЕТЕ ВНИМАТЕЛНИ: Не одговарајте на сомнителна е-пошта, не следете ги линковите од сомнителна е-пошта или пораки и не отворајте прилози! Не кликнувајте на линкот, туку внесете ја адресата во вашиот прелистувач! Не одговарајте на пораки каде што некој бара од вас да му испратите банкарски пин, лозинки, копии од вашата лична карта или други доверливи лични податоци! Не пополнувајте обрасци со вашите лични податоци на сомнителни и непроверени веб страници!

3) КРАЖБА НА ИДЕНТИТЕТ

Еден од начините на злоупотреба на личните податоци со најсериозни последици за поединецот е кражба на идентитет. Кражба на идентитет е чин со кој некој користи (собира, обработува) лични податоци на поединец спротивно на законот. Тоа претставува повреда на Законот за заштита на личните податоци, но исто така е **кривично дело** за кое е предвидена и казна затвор до една година.

Примери: Вашите лични податоци може да бидат злоупотребени на таков начин што лице кое сака да му наштети на вашиот углед и чест и да ја наруши вашата приватност отвора лажен профил на социјалните мрежи во ваше име и на тој профил објавува содржини со вулгарен или навредлив карактер.

Измамникот создава **лажен профил имитирајќи вистинска личност**, вклучувајќи фотографии, занимање и други детали, за да ја зголеми веројатноста во стекнување на доверба на поединци кои сака да ги измами. Тој испраќа директна порака која содржи врски до други веб страници или злонамерен код интегриран во веб линкот која што краде лични податоци. Крајната цел е да се искористи довербата на корисникот за да побара пари или други информации што може да бидат профитабилни.

4) ШПИОНСКИ СОФТВЕР

Шпионски софтвер (spyware) **е штетен софтвер кој ги „шпионира“ вашите активности на интернет и ги собира вашите лични податоци додека** „adware“ **е рекламен софтвер кој исто така инсталира скокачки прозорци и реклами**. Креаторите на рекламни софтвери и дистрибутерит е заработуваат пари од трети страни преку овие начини: добиваат пари секој пат кога отворате реклама, добиваат пари секој пат кога ќе ви се прикаже реклама или добиваат пари секој пат кога ќе се инсталира софтверски пакет на уредот. Рекламниот софтвер исто така може да ја следи вашата историја на пребарување и прелистување за да прикажува реклами што се порелевантни за вас. Штом програмерот ќе ја добие вашата локација и историјата на прелистувачот, може да заработи дополнителен приход со продажба на тие информации на трети страни. Покрај тоа, шпионскиот софтвер може да биде злонамерен и да го скенира вашиот хард диск, да ги украде вашите лични податоци како банкарските податоци и лозинките.

Пример: „PhoneSpy“ е пример за шпионски вирус кој се преправа дека е мобилна апликација за да добие пристап и да зарази андроид мобилни уреди. Овој пристап им овозможува на закануваче далечински да ги контролираат мобилните уреди и да крадат податоци.

„Pegasus“ е најновиот пример за тоа колку сите сме ранливи во однос на дигиталното љубопитство. Нашите телефони ги чуваат нашите најлични информации, вклучувајќи фотографии, текстуални пораки и е-пошта. Шпионскиот софтвер може директно да открие што се случува во нашите животи, заобиколувајќи ја крипцијата што ги штити податоците испратени преку интернет. „Pegasus“ е најмоќната хакерска алатка досега измислена. Развиен е од израелска компанија и дизајниран да го напаѓа речиси секој паметен телефон. Може тајно да го претвори мобилниот телефон во уред за 24-часовен надзор и да добие пристап до сите информации од телефонот, да чита пораки и да презема фотографии, да слуша и снима гласовни и видео повици. Може да се користи за да се претставува како жртвата и да добие пристап до дигитални и физички средства.

5) ИЗМАМИ ПРИ КУПУВАЊЕ ИЛИ ПРОДАВАЊЕ НА ИНТЕРНЕТ

Сите измами во оваа категорија на измами се основаат на убедување на жртвата да се вклучи во наводни правни трансакции. Измамниците нудат одлични производи за многу ниски цени.

БИДЕТЕ ВНИМАТЕЛНИ: кога нешто е премногу добро за да биде вистинито, речиси секогаш е измама. Жртвата се уверува дека по плаќањето ќе го добие производот што го купила, но тоа не се случува. Исто така, постојат измами кога целта е да се украдат личните податоци на жртвата.

Примери: лажни веб страници за интернет купување на електроника, автомобили, станови итн. „Фишинг“ напади каде целта е да ги украдат вашите лични податоци и да ги злоупотребат.

6) ЛАЖНА Е-ПОШТА ВО КОЈА СЕ ТВРДИ ДЕКА СТЕ НАСЛЕДИЛЕ ПАРИ, СТЕ ДОБИЛЕ НА ЛОТАРИЈА ИЛИ СТЕ ДОБИЛЕ НАГРАДА

Измамата обично започнува со барање да исплатите мала надокнада за да помогне во правните процеси и документацијата, ветувајќи ви голема сума пари која ќе ја добиете потоа (т.е. богато нигериско семејство или поединец кој сака да го сподели своето богатство во замена за помош за пристап до нивното наследство).

Измамникот неизбежно ќе бара пообемни такси за покривање на понатамошни административни задачи и трансакциски трошоци поддржани со документи за потврда со легитимен изглед. Сепак, ветениот повратна инвестицијата никогаш не пристигнува.

Примери: Добивте е-пошта во која се тврди дека сте добиле на лотарија. Сè што треба е да ги испратите вашите лични податоци, да платите мала надокнада и ќе ги добиете вашите пари.

Добивте порака во сандачето на Фејсбук дека сте добиле пари на награден натпревар. Само треба да испратите копија од лична карта и фотографија за да можете да ја подигнете наградата.

Добивте е-пошта во која се тврди дека сте наследиле пари од вујко од Австралија за кој не сте ни знаеле дека постои. Само треба да платите за некои административни трошоци.

7) ВЕ СЛЕДАТ, А ВАШИТЕ ЛИЧНИ ПОДАТОЦИ СЕ КОРИСТАТ И СПОДЕЛУВААТ БЕЗ ТОА ДА ГО ЗНАЕТЕ

Кога се инсталира апликација, од корисниците често се бара да имаат дозвола за пристап до камерата, датотеките или микрофонот. Сето горенаведено може да доведе до злоупотреба на личните податоци кои ви се зачувани во уредот. Размислете добро пред да дозволите таквите апликации да пристапат до вашите лични податоци! **Никогаш не инсталирајте апликации од непознати и непроверени извори**!

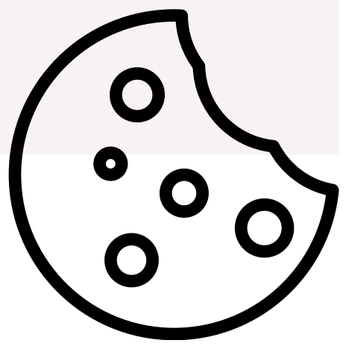
Дали ги читате политиките за приватност на веб страниците што ги посетувате и на социјалните мрежи што ги користите? Или само кликате на копчето „Се согласувам“ за да исчезнат тие досадни известувања за приватност за да можете мирно да продолжите да пребарувате на интернет или да ја користите саканата услуга? Мислите дека тоа е добра идеја? Дали сакате другите да профитираат од вашите лични податоци?

Во свет управуван од податоци, големите технолошки компании, платформите за социјални мрежи, пребарувачите, добавувачите на софтверски решенија, брокерите за податоци и други го базираат својот профит на собирање на вашите лични податоци и нивно споделување со трети страни. Тие исто така можат да ја следат вашата е-пошта, пребарувањата, локациите, страниците што ве интересираат, што „сакате“ на социјалните мрежи. Тие ве следат користејќи колачиња и други технологии за следење. **Колачињата се мали датотеки кои што веб прелистувачот ги складира на компјутер, мобилен уред или друг уред кога корисникот ја посетил веб страницата. Чувањето колачиња на вашите уреди е дозволено само со ваша согласност и претходно јасно известување кои податоци ќе се собираат и за каква цел, а во согласност со прописите за заштита на личните податоци.** Само колачињата кои се технички неопходни за нормално функционирање на страницата или за обезбедување на услугата на барање на корисникот немаат потреба од согласност.

Известувањата за колачиња што се појавуваат на веб страницата често се нејасни, долги и тоа со причина: да ве обесхрабрат да ги читате и да кликнете „Прифати ги сите“.

БИДЕТЕ ВНИМАТЕЛНИ: пред да прифатите колачиња, внимателно прочитајте кои колачиња ги користи страницата, за какви цели ги користи! Многу веб страници користат рекламни колачиња за да ви прикажуваат целно насочени реклами и да ги споделат вашите лични податоци со трети страни.

На прв поглед, вредноста на „лајкот“ на социјалната мрежа не изгледа дека има големо значење. Меѓутоа, ако овие навидум безвредни податоци се споени со други лични податоци собрани преку колачиња и друга технологија за следење, тие може да се користат за создавање на профил на поединец, идентификување на неговите или нејзините политички преференции, целно рекламирање за ширење на лажни вести и погрешни информации и/или да се влијае врз мислите и постапките на поединците. На пример, можно е да се убеди лице да гласа за одредена политичка партија преку испраќање на целно насочени пораки преку социјалните мрежи специјално прилагодени на тоа лице врз основа на креираниот профил.



КАКО ДА ГИ ЗАШТИТИТЕ ВАШИТЕ ЛИЧНИ ПОДАТОЦИ ОД КРАЖБА И ЗЛОУПОТРЕБА?

1. Периодично креирајте сигурносна копија на податоците на надворешна меморија или облак.
2. Задолжително користете антивирусни програми и редовно ажурирајте ги и надградувајте ги антивирусните и други безбедносни алатки.
3. Надградете ги и ажурирајте ги оперативните системи и сите апликации на вашиот компјутер со најновите верзии.
4. Не отворајте е-пошти што пристигнуваат од сомнителни адреси, невообичаени домени, особено не отворајте сомнителни прилози на е-пошти кои имаат невообичаена форма, содржат невообичаени изрази, имаат многу граматички грешки или текстот делува како лош превод или не во духот на македонскиот јазик (на пр. „прикачен е на вашето читање“).

5 Проверете го испраќачот на е-поштата пред да ја отворите. Ако идентитетот на вашиот испраќач е сомнителен, не отворајте ја е-поштата! (пр. amagnus@india.com).

6 Обрнете внимание на екстензијата на датотеката во прилогот, не отворајте прилози со необични екстензии како што се as.jar,.ace.

7 Ако е-поштата што ја добивте содржи сомнителна URL-адреса, поминете со глувчето преку URL-адресата во поштата, но не кликнувајте! Треба да ја видите вистинската URL адреса на која ќе бидете пренасочени. Ако изгледа сомнително или завршува како.exe,.js или .zip, не отворајте го линкот!

8 Кога ќе завршите со користењето на вашиот профил на социјалната мрежа, е-пошта или друга услуга на интернет, одјавете се. Ако останете најавени и продолжите да сурфате, тоа е исто како да ја оставите отклучена вашата куќа: им ја олеснувате работата на хакерите и уценувачите. Затоа, избегнувајте ги ризиците и одјавете се од вашите сметки пред да продолжите да ја прелистувате веб страницата!

9 Внимавајте на понуди кои се „премногу добри за да бидат вистинити“ на непроверени и непознати е-продавници. Купувајте само во проверени е-продавници, читајте рецензии, ако плаќате со кредитна картичка плаќајте само преку проверени даватели на услуги за плаќање, бидете многу внимателни ако некој ве замоли да му ги испратите вашите лични податоци или ви испрати линк до сомнителни веб страници! Ова може да биде „фишинг“ напад со цел да се украдат вашите лични податоци и вашите пари!

10 Кога плаќате на интернет, не користете отворена или бесплатна Wi-Fi (Вај-фај) мрежа, туку користете само безбедна Wi-Fi мрежа.

Оваа публикација е изработена како дел од твининг-проектот „Поддршка во спроведувањето на модернизираната правна рамка за заштита на личните податоци“, финансиран од Европската Унија. Содржината на публикацијата е единствена одговорност на авторите и на проектните партнери, и не може да се смета дека ги одразува ставовите на Европската Унија.

Побарајте повеќе информации на www.azlp.mk

SCAN ME

Овој проект е финансиран од Европската Унија