Digital Security
Progress. Protected.

Ako zostať na internete v bezpečí?

Príručka digitálnej bezpečnosti
pre všetky generácie

Obsah:

Vďaka informáciám v tejto brožúrke zostanete o krok vpred pred kybernetickými zločincami. Aktuálne informácie zo sveta digitálnej bezpečnosti nájdete na stránke **Bezpečne na nete**.

Bezpečne na nete.sk

O príručke, ktorú držíte v rukách

Milí čitatelia,

technológie sa stali prirodzenou súčasťou našich každodenných životov. Vďaka nim môžeme byť bližšie k rodine, zjednodušujú naše každodenné aktivity a otvárajú nám nové možnosti. Spolu s týmito výhodami však prichádzajú aj riziká, ktoré môžu ohroziť naše osobné údaje alebo financie.

Podvodníci, žiaľ, zneužívajú skutočnosť, že najmä staršie ročníky nevyrastali s technológiami tak ako dnešní tínedžeri. Mladí, naopak, často a vedome prehliadajú riziká, ktoré na nich číhajú na internete. A v podstate všetci sme zraniteľní vo chvíľach, keď nie sme ostražití. Napríklad, keď si pre dnešnú uponáhľanú dobu nenájdeme ani chvíľku na to, aby sme sa zamysleli, či e-mail, ktorý sme práve dostali, je autentický alebo ide o podvod.

Aj keď sa digitálny svet môže niekedy javiť zložitý a neznámy, nemalo by nám to brániť vo využívaní jeho predností. Moderné technológie sú tu na to, aby nám uľahčili život. Ak si každý bez ohľadu na vek osvojí základné pravidlá digitálnej bezpečnosti, budeme môcť všetci využívať moderné technológie bez väčších obáv.

Radi by sme vám v tom pomohli. Preto sme s kolegami, odborníkmi na digitálnu bezpečnosť, vytvorili krátku príručku digitálnej bezpečnosti, ktorá nielen vám, ale aj vašim blízkym pomôže lepšie porozumieť tomu, ako byť pri používaní internetu v bezpečí. Ponúka jednoduché rady a praktické tipy, vďaka ktorým budete vedieť, ako sa bezpečne pohybovať na internete, chrániť svoje údaje a rozpoznať internetové podvody.

Veríme, že sa budete s našimi radami cítiť istejšie a bez obáv využijete všetky benefity, ktoré digitálny svet ponúka. A najlepšie bude, ak si ju prečítate aj s rodinou, aby ste boli spoločne online všetci v bezpečí.

Ondrej Kubovič
špecialista na digitálnu bezpečnosť, ESET

Bezpečnosť zariadenia

Mnohé domácnosti dnes využívajú aj viacero digitálnych technológií denne, ktoré sú pripojené na internet a obsahujú citlivé informácie vrátane bankových údajov či fotografií. Od počítačov cez mobilné telefóny až po inteligentné zariadenia. S veľkým počtom zariadení sa zvyšuje šanca, že sa používateľ stane terčom kybernetického útoku. Dodržiavanie základných pravidiel digitálnej bezpečnosti dokáže toto riziko výrazne znížiť.

Základné pravidlá zabezpečenia počítača

Aktualizácie

Udržiavajte svoj operačný systém aj všetky aplikácie v najaktuálnejšej verzii. Aktualizácie opravujú bezpečnostné chyby, cez ktoré sa útočníci dokážu infiltrovať do zariadenia.

Bezpečnostný softvér

Používajte antivírusový program, ktorý dokáže škodlivý kód eliminovať ešte pred tým, ako napácha škody v zariadení. Taktiež nezabúdajte aktualizovať aj bezpečnostný softvér.

Firewall

Aktivujte na svojom zariadení firewall, ktorý zabráni útočníkom v neoprávnenom prístupe k vašej sieti. Ide o systém na kontrolu toku dát medzi vaším počítačom a internetom.

Sťahujte len z overených zdrojov

Všetky programy a súbory sťahujte iba z oficiálnych zdrojov. Obsah získaný z pochybných zdrojov môže obsahovať škodlivý kód. Taktiež sa vyhýbajte nelegálnym stránkam a obsahu.

Silné heslá

Používajte silné a unikátne heslá pre všetky účty spolu s dvojfaktorovou autentifikáciou. Ak sa útočníci dostanú do vášho účtu, môžu vaše zariadenie infikovať škodlivým kódom.

Zabezpečenie routra

Prvým krokom je zmena predvoleného hesla vášho routra od dodávateľa po jeho zakúpení. Tieto heslá bývajú často verejne známe. Zvyšuje sa tým pravdepodobnosť, že ho útočníci ľahko uhádnu, prihlásia sa do routra, zmenia jeho nastavenia a ohrozia vaše pripojenie do domácej siete. Nezabúdajte tiež na aktualizácie softvéru a firmvéru.

Rozmýšľajte, kým kliknete

Buďte opatrní pri otváraní e-mailov a odkazov z neznámych zdrojov. Nikdy neposielajte citlivé údaje, ako sú heslá, prostredníctvom e-mailu.

Zálohovanie

Pravidelne vykonávajte zálohy svojich dát na externé úložiská, ideálne v cloude aj na fyzických nosičoch. V prípade infikovania zariadenia tak neprídete o dôležité súbory.

Základné pravidlá zabezpečenia mobilných zariadení

Pri zabezpečení mobilných telefónov a tabletov sa treba držať odporúčaní, ktoré platia aj pre počítače. Mobilné zariadenia však majú aj svoje špecifiká.

Fyzické zabezpečenie zariadenia

Dôležitá je ochrana zariadenia fyzickým obalom pre prípad pádu alebo poškodenia. Na verejných miestach majte mobil vždy pri sebe a nenechávajte ho bez dozoru.

Zabezpečenie softvérom

Zariadenie ochráňte bezpečnostným softvérom s funkciou Anti-Theft, ktorá dokáže vyhľadať odcudzené alebo stratené zariadenie a vyhotoviť fotografiu zlodeja. Takisto povoľte vymazanie obsahu mobilu na diaľku.

Prístup do zariadenia

Používajte uzamykanie displeja s PIN kódom, odtlačkom prsta alebo skenom tváre. Takisto si nastavte čas, po ktorom sa zariadenie v prípade nečinnosti automaticky uzamkne. Odporúča sa aj zmena predvoleného PIN kódu SIM karty.

Pozor na aplikácie z neoficiálnych obchodov

Aplikácie sťahujte iba z oficiálnych obchodov (Google Play pre Android, App Store pre iOS) alebo priamo od poskytovateľa služby.

Aktualizácie všetkých aplikácií

Ubezpečte sa, že máte aktualizované všetky nainštalované aplikácie. Zároveň si nastavte ich automatické aktualizácie.

Povolenia

Všímajte si, aké povolenia si od vás pýta aplikácia. Ak sa vám zdá, že sú pre účel aplikácie neadekvátne, nesťahujte aplikáciu.

Bezpečné pripojenie

Vyhnite sa pripájaniu k neznámym alebo verejným nezabezpečeným Wi-Fi sieťam. Pri práci s citlivými dátami sa radšej pripojte na mobilné dáta.

Tip: Odporúčame vám, aby ste mali aktivované služby, ktoré vám umožnia zariadenie na diaľku nájsť, uzamknúť či vymazať. Ide o výbornú funkciu, ktorá môže ochrániť vaše súkromie v prípade, ak zariadenie stratíte alebo vám ho niekto ukradne.

Škodlivý kód

Jednou z najznámejších digitálnych hrozieb je škodlivý kód, inak povedané malvér. Ide o druh softvéru, ktorý dokáže spôsobiť problémy na infikovanom zariadení, pričom môže napadnúť počítač, smartfón aj tablet. Podľa toho, o aký typ škodlivého kódu ide, dokáže kradnúť osobné informácie, poškodiť súbory alebo dokonca prevziať kontrolu nad vaším zariadením.

Najbežnejšie druhy škodlivého kódu

Ransomvér získa a zablokuje prístup k vašim súborom a požaduje výkupné za ich odblokovanie alebo nezverejnenie.

Trójsky kôň sa maskuje ako neškodný program, no v skutočnosti ide o škodlivý kód, ktorý môže poškodiť počítač alebo získavať osobné údaje.

Spyvér je navrhnutý na sledovanie aktivít obete a získavanie osobných informácií bez jej vedomia.

Keylogger zaznamenáva stlačenia na klávesnici, čím umožňuje útočníkovi odchytávať komunikáciu alebo prihlasovacie údaje. Dokáže tak ukradnúť aj dáta, ktoré obeť nemá nikde uložené.

Password stealer sa zameriava výhradne na súbory či programy, ktoré by mohli obsahovať heslá k rôznym službám a tie sa snaží ukradnúť.

Bankový malvér je špeciálny typ škodlivého kódu navrhnutý na krádež bankových informácií a finančných údajov vrátane čísla karty alebo prístupu do bankového účtu či kryptopeňaženky.

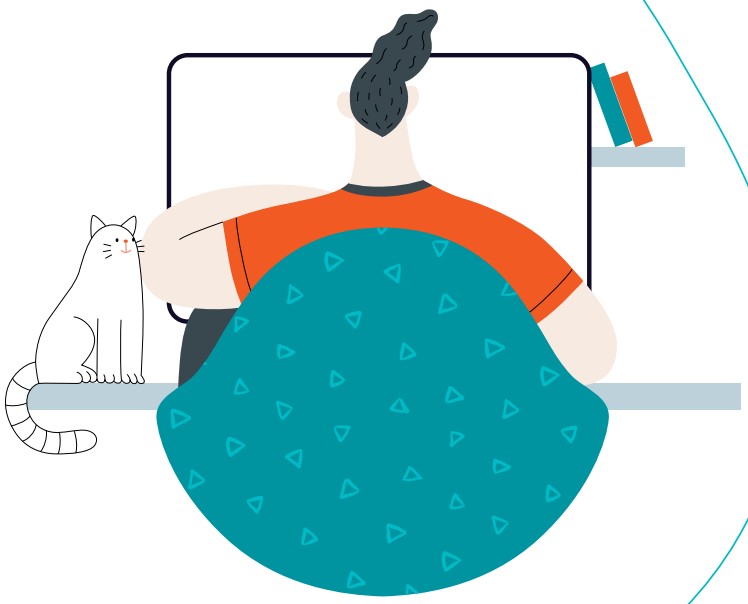
Advér zobrazuje nežiaduce reklamy na zariadení a môže spomaliť jeho výkon. Najčastejšie sa prejavuje ako množstvo nevyžiadaných vyskakovacích okien na webovej stránke.

Červ má schopnosť replikovať sa z nakazeného počítača sám od seba bez potreby akéhokoľvek zásahu zo strany človeka.

Škodlivý kód na ťažbu kryptomien využíva výpočtový výkon počítača obete na ťažbu kryptomien bez jej súhlasu.

Ako sa najčastejšie šíri škodlivý kód?

- Cez infikované prílohy v e-mailoch
- Webové prehliadače
- Skompromitované webové stránky
- Vyskakovacie okná
- Četovacie služby
- Sociálne siete
- Zraniteľnosti
- Nástroje, ktoré slúžia na sťahovanie obsahu



Znaky upozorňujúce na prítomnosť škodlivého kódu

1. Zariadenie je spomalené.
2. E-mailová schránka je zaplnená správami bez odosielateľa alebo predmetu.
3. Pretrváva problém s prístupom na internet.
4. Na webových stránkach sa zobrazuje množstvo reklám.
5. Bezpečnostný softvér upozorňuje na zachytenú hrozbu.

Dobré vedieť: Upozorňujeme, že niektoré spomenuté znaky nemusia vždy znamenať prítomnosť škodlivého kódu, napríklad spomalené zariadenie. Môže ísť o problém so zastaraným operačným systémom alebo neaktualizovaným softvérom. Napriek tomu je dôležité tieto príznaky neignorovať a byť obozretní. Pre zaistenie maximálnej úrovne ochrany vašich dát a súkromia je nevyhnutné používať kvalitný bezpečnostný softvér.

Ako vám pomôže bezpečnostný softvér?

V minulosti slúžili takzvané antivírusy primárne na blokovanie infikovaných súborov. Dnes je škála kybernetických hrozieb omnoho širšia, čomu sa prispôsobila aj digitálna ochrana. Dnešné bezpečnostné riešenia sú komplexné, zložené z viacerých vrstiev ochrany, ktoré nielen zachytávajú, blokujú a odstraňujú škodlivý kód, ale rovnako chránia používateľov pred ďalšími kybernetickými hrozbami, akými sú rôzne sofistikované útočné techniky či phishingový útok.

1. Pôsobí ako štít pred škodlivým kódom

Bezpečnostný softvér deteguje, odstraňuje a predchádza kybernetickým hrozbám. Riešenie sa stará o to, aby škodlivý kód nemal pootvorenú bránu do vášho zariadenia napríklad slabým zabezpečením Wi-Fi siete.

2. Chráni vás pri vašich online aktivitách

Bezpečnostný softvér chráni vaše osobné údaje a informácie. Ochráni vás pri online nákupoch aj prehliadaní webových stránok.

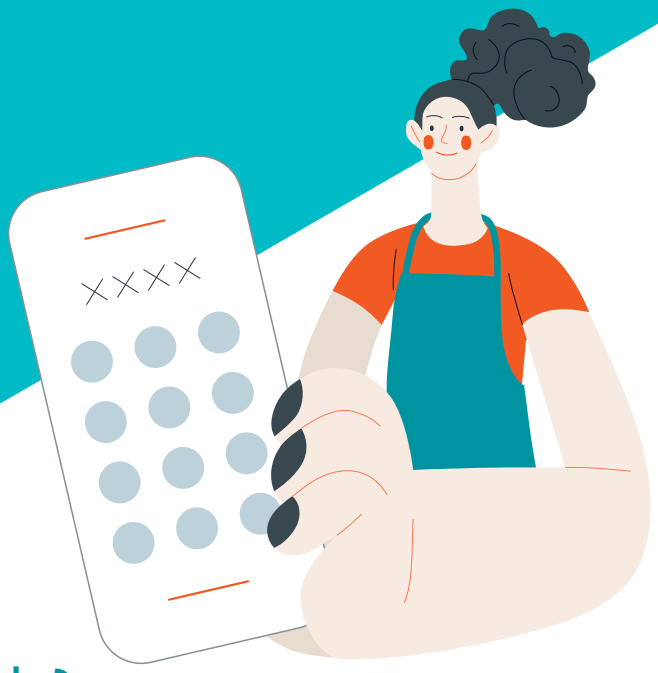
3. Zabezpečí všetky vaše zariadenia

Dnes je potrebné chrániť všetky zariadenia, ktoré pripájate k internetu, či už je to počítač, smartfón, inteligentná TV alebo tablet.

Dobré vedieť: Vaše zariadenie môže byť infikované aj v prípade, ak váš počítač nepripájate k internetu. Ako sa to môže stať? K zariadeniu môžete pripojiť napríklad USB kľúč, ktorý v sebe obsahuje škodlivé súbory. Pomocníkom v tomto prípade môže byť opäť bezpečnostný softvér, ktorý skontroluje každé takéto externé zariadenie pripojené k počítaču.

Heslá

Heslá slúžia v digitálnom svete ako kľúč na ochranu dôležitých informácií a prístupov. Ich úlohou je zabezpečiť, aby sa k zariadeniam, účtom a citlivým údajom dostali len oprávnení používatelia. Využívanie silných hesiel je preto mimoriadne dôležité v prevencii pred rôznymi digitálnymi hrozbami.



Prečo je zaujímavé aj vaše heslo?

Ak si myslíte, že nie ste pre útočníkov zaujímavý terč, mýlite sa. Každý z nás dnes vlastní niečo cenné. Okrem peňazí sú pre útočníkov cenným tovarom vaše súkromné údaje.

Finančný zisk

Útočníci môžu vaše získané heslo predať na čiernom trhu. Kupujúci (ďalší útočníci) potom môžu tieto údaje zneužiť na vlastné kriminálne účely, napríklad vydieranie či krádež vašej identity.

Preniknutie do účtov s platobnými údajmi

Kyberzločinci môžu zneužiť prihlasovacie údaje aj na preniknutie do účtov s vašimi platobnými údajmi a získať tak informácie o vašej platobnej karte.

Preniknutie do účtov na sociálnych sieťach

Útočníci môžu získať kontrolu nad celým vaším účtom a použiť ho na krádež vašej identity alebo šírenie podvodných kampaní medzi vašimi priateľmi.

Ako môžu útočníci získať vaše heslo?

- Uhádnutím slabého hesla
- Fyzickým odsledovaním hesla
- Podvodnou správou
- Vylákaním na falošnej stránke
- Odchytávaním sieťovej komunikácie
- V rámci úniku údajov slabo zabezpečenej služby
- Škodlivým kódom na krádež hesiel

Pridajte k heslu aj dodatočné overenie

Väčšina online služieb, ktoré používate, ponúka ochranu vášho účtu aj v prípade, keď útočníci získajú vaše heslo. Ide o bezpečnostnú poistku dodatočným overením, takzvanú **dvojfaktorovú autentifikáciu**.

Po úspešnom zadaní hesla si služba v rámci overenia, že ide naozaj o oprávnenú osobu, vypýta údaj, ktorým disponuje iba ona. Môže ísť o zaslanie jednorazového kódu do SMS správy, overenie totožnosti v inej online službe alebo na inom zariadení či autentifikácia prostredníctvom špeciálnej aplikácie.

Ako vytvoriť silné heslo?

1. Neobsahuje informácie o vás

Útočníci môžu skúšať uhádnuť heslo cez znaky a slová, ktoré majú s vami spojitosť. Príkladom je dátum narodenia alebo meno vášho domáceho miláčika.

2. Heslo je jedinečné pre každý účet

Je potrebné, aby ste používali jedinečné heslo do každého účtu. Ak útočníci získajú vaše heslo, môžu ho skúšať použiť aj v rámci ostatných služieb.

3. Heslo je dostatočne dlhé

Odporúčaná dĺžka hesla je 8 až 16 znakov.

4. Heslo obsahuje prístupovú frázu

Namiesto klasického hesla použite krátku vetu, ktorú si ľahko zapamätáte. Prístupové frázy sú často oveľa dlhšie ako bežné heslo, a preto sú spravidla silnejšie.

6. Vyhýbajte sa často používaným slovám

Dobré heslo alebo prístupová fráza neobsahuje často používané slová, ako je napríklad „heslo".

7. Nepoužívajte opakujúce sa znaky

Dobré heslo neobsahuje opakujúce sa a sekvenčné znaky, ako je napríklad „1111", „1234" alebo „abab".

Ako si zapamätať množstvo zložitých hesiel?

Pokiaľ používate viacero online účtov a je pre vás náročné zapamätať si heslo ku každému z nich, pomôcť vám môže správca hesiel. Ide o softvér špeciálne navrhnutý na vytváranie silných hesiel a ukladanie prihlasovacích údajov. Správca hesiel dokáže uložiť celé zoznamy hesiel a takýto zoznam chráni nielen ďalším heslom, ale aj šifrovaním. Vďaka nemu budete potrebovať len jediné – hlavné heslo – ostatné si už nemusíte pamätať.

Bezpečnosť prehliadača

Internetový prehliadač je program, ktorý slúži na prehliadanie obsahu na internete. Medzi najznámejšie patria Google Chrome, Mozilla Firefox, Safari či Microsoft Edge. Prehliadače obsahujú obrovské množstvo citlivých informácií. Od histórie prehliadania cez heslá až po údaje o kreditných kartách. Preto nie je prekvapením, že môžu byť zneužité útočníkmi a to nielen na šírenie škodlivého kódu.

Ako vyzerajú útoky cez prehliadač?

Škodlivé rozšírenia prehliadača

Rozšírenia sú doplnky, ktorými môžete obohatiť funkcionalitu vášho prehliadača, napríklad pridaním nástroja na blokovanie reklám alebo prekladanie textu. Prostredníctvom škodlivých rozšírení, ku ktorých stiahnutiu vás môžu zmanipulovať podvodom útočníci, si však môžete infikovať zariadenie škodlivým kódom.

Zneužitie zraniteľnosti

Útočník môže zneužiť zraniteľnosť v prehliadači alebo v jeho rozšírení na infikovanie zariadenia. V takomto prípade stačí, že navštívite skompromitovanú stránku. Je preto dôležité vždy používať aktualizovanú verziu prehliadača a všetkých doplnkov.

Útočník v prehliadači

Pri útoku man-in-the-browser už bolo zariadenie obete infikované škodlivým kódom, ktorý umožňuje prístup do zraniteľného prehliadača. Tento škodlivý kód odchytáva údaje, ktoré zadávate na webovej stránke, ako číslo kreditnej karty, prihlasovacie meno a heslo alebo stránku upravuje podľa zadania útočníka, ktorému posiela informácie.

Škodlivý kód ťažiaci kryptomeny

Útočníci môžu zneužiť váš prehliadač aj na ťažbu kryptomeny. Problém sa prejaví najmä viditeľným znížením výkonu zariadenia.

Falošné webové stránky

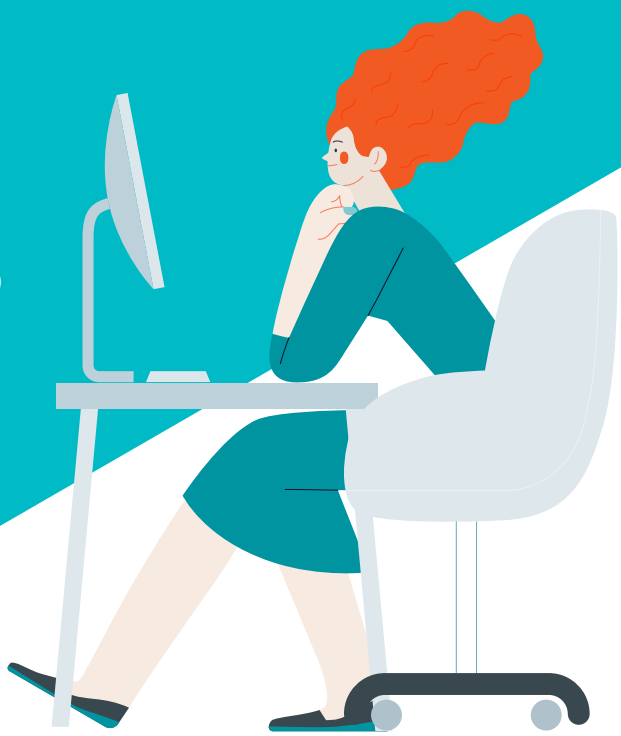
Podvodníci vás môžu nalákať na rôzne falošné stránky, ktoré sú na prvý pohľad na nerozoznanie od webu vašej banky alebo sociálnej siete. Na takýchto stránkach môžete nevedomky útočníkom odovzdať svoje prihlasovacie údaje alebo si do zariadenia stiahnuť škodlivý kód.

Ako rozpoznať nebezpečnú stránku?

- V URL adrese na začiatku v časti https chýba písmeno s. Znamená to, že komunikácia s webom nie je šifrovaná.
- Na stránke sú gramatické a štylistické chyby.
- Chýba kontakt na prevádzkovateľa webu.
- Stránka obsahuje až príliš lákavé ponuky a veľa blikajúcich okien.
- Stránka vás vyzýva k okamžitej akcii.

Čo robiť, ak sa dostanete na nebezpečnú webovú stránku?

Ak sa dostanete na podozrivú stránku, neklikajte na žiadne prvky, ktoré obsahuje (tlačidlá, obrázky, odkazy) a stránku čo najskôr opustite a zavrite. Pre vyššiu bezpečnosť následne svoje zariadenie preskenujte spoľahlivým bezpečnostným softvérom, ktorý by mal detegovať, zneškodniť a odstrániť prípadné hrozby, ktoré ste si mohli pri návšteve webu stiahnuť.



Ako sťahovať z internetu bezpečne?

Využívajte stránky oficiálnych vývojárov

Ak si chcete stiahnuť nový program, využite na to oficiálnu webovú stránku samotného vývojára softvéru (napr. Microsoft alebo overené e-shopy) alebo oficiálne internetové obchody (Google Play, Apple AppStore).

Kliknutie si dvakrát premyslite

Mnohé z odkazov môžu viesť k podvodným alebo škodlivým stránkam.

Používajte spoľahlivé bezpečnostné riešenie

Kvalitný bezpečnostný softvér automaticky spustí kontrolu pre každý sťahovaný súbor a zablokuje všetky nebezpečné položky, čím chráni vaše zariadenie.

Ako môžete zvýšiť bezpečnosť prehliadača?

1. Používajte firewall.
2. V nastaveniach prehliadača zapnite funkciu „safe browsing“.
3. V nastaveniach prehliadača vypnite automatické otváranie okien.
4. Všímajte si, či má stránka zabezpečené pripojenie. Na začiatku URL adresy by sa malo nachádzať v časti https písmeno s.
5. Aktualizujte internetový prehliadač.
6. Používajte dôveryhodné rozšírenia prehliadača.
7. Používajte kvalitný bezpečnostný softvér.
8. Využite pripojenie cez službu VPN, ktorá dokáže vytvoriť šifrovaný tunel medzi zariadením a stránkou.

Online nakupovanie

Nakupovanie cez internet je čoraz obľúbenejšie. Bohužiaľ, všetko, čo sa teší popularite, je atraktívne pre kybernetických zločincov. Je preto potrebné poznať praktiky podvodníkov, ktorými sa to v online svete hemží. Môžete tak ochrániť vaše peniaze a zaručiť, že dostanete to, za čo platíte.

Najčastejšie hrozby, na ktoré si treba dávať pozor pri nakupovaní

Podvodné reklamy – po kliknutí na takúto reklamu vás presmeruje na stránku s podvodným obsahom, ktorá môže propagovať falošný tovar.

Falošné webové stránky majú veľa podôb. Napríklad by sa mohlo zdať, že renomovaný e-shop spustil samostatnú doménu na umiestnenie svojich ponúk pre vianočné výpredaje.

Falošné darčekové karty a kupóny – ak vás falošný kupón zláka a kliknete naň, do vášho zariadenia si môžete stiahnuť škodlivý kód.

Podvodné aplikácie – útočníci pri cielení na používateľov mobilných aplikácií vytvárajú podvodné aplikácie, ktoré pôsobia ako legitímne e-shopy.

Phishingové útoky – zločinec vám môže poslať e-mail, ktorý sa tvári ako zákaznícka podpora internetového obchodu a hovorí vám, že došlo k problému s vašou objednávkou a vyzvať vás k poskytnutiu údajov z karty.

Podvody na internetových bazároch

Samostatnou kapitolou sú podvody na online bazároch, kde predajcom môže byť každý. Medzi najčastejšie podvody patrí inzerovanie chybných produktov alebo falzifikátov či nedoručenie tovaru po zaplatení. Obeťou sa však môžu stať aj predávajúci. Obľúbenou taktikou pri falošnej transakcii je odkaz na stránku fiktívnej platobnej alebo kuriérskej služby, kde má obeť potvrdiť záujem o prijatie platby zadaním údajov o platobnej karte. Ich získaním útočníci dokážu vykonávať platby v mene obete.

Čo robiť, ak ste nakúpili cez falošný internetový obchod?

- Ak ste na webe falošného obchodu odovzdali informácie o svojej platobnej karte, **bezodkladne sa spojte s bankou** a požiadajte ju o zablokovanie karty. Tento krok môžete vykonať aj cez aplikáciu vašej banky, pokiaľ ponúka takú možnosť.
- Preskenujte si zariadenie na prítomnosť škodlivého kódu a zmeňte si prihlasovacie údaje v prípade, že ste ich odovzdali útočníkom.
- Ak ste za tovar zaplatili, ale nebol vám doručený, alebo vám prišiel falzifikát, môžete podať podnet na Slovenskú obchodnú inšpekciu.
- Ak ste utrpeli finančnú ujmu, spojte sa s políciou.

Upozornenie: Ak útočníci získali vaše prihlasovacie údaje, okamžite ich zmeňte. Najskôr však vaše zariadenie preskenujte na prítomnosť škodlivého kódu. Ak si zmeníte heslo skôr a vaše zariadenie bolo infikované napríklad škodlivým kódom s názvom keylogger, ktorý sleduje, čo píšete na klávesnici, útočníci sa dostanú aj k vášmu novému heslu. Zmenu prihlasovacích údajov odporúčame vykonať aj v prípade ďalších služieb, ktoré neboli priamo ohrozené. Útočníci vedia, že používatelia používajú tie isté heslá do rôznych služieb.

Ako nakupovať na internete bezpečne?

1. **Vždy nakupujte zo zariadenia, ktoré je zabezpečené** bezpečnostným softvérom a z bezpečného internetového pripojenia. Pri nákupoch sa vyhnite verejným Wi-Fi.
2. **Skontrolujte si zabezpečenie internetovej stránky e-shopu** overením, či sa adresa webovej stránky začína na „https://".
3. **Overte si údaje o prevádzkovateľovi e-shopu** (sídlo, fakturačné informácie, IČO, DIČ, kontaktné informácie).
4. **Pozorne si prečítajte** všeobecné obchodné a reklamačné **podmienky**.
5. **Registrácia k nákupu nie je vždy potrebná**. Ak sa aj napriek tomu rozhodnete účet vytvoriť, použite jedinečné a silné heslo.
6. Ak od vás obchodník vyžaduje **ďalšie informácie**, ako sú informácie **o svojom bankovom účte, číslo OP** či **heslá**, okamžite obchod opustite.
7. Akýkoľvek e-shop, ktorý sľubuje **príliš veľa za príliš nízku cenu**, je podozrivý a s najväčšou pravdepodobnosťou falošný.
8. Pri identifikovaní toho, či je e-shop bezpečný, vám môžu pomôcť aj **recenzie samotných používateľov** na konkrétnom e-shope alebo na stránkach, akou je napríklad Heureka.sk.
9. Použiť kreditnú kartu alebo radšej platbu na dobierku? Pokiaľ si stále nie ste istí, zvoľte **platbu na dobierku**, ktorú poskytuje väčšina online predajcov.

Elektronická komunikácia

Elektronická komunikácia sa stala neoddeliteľnou súčasťou moderného spôsobu života. Poskytuje rýchly a efektívny spôsob komunikácie medzi jednotlivcami či skupinami. V mnohých prípadoch sú četovacie aplikácie či e-maily vstupnou bránou, cez ktorú sa môžu útočníci dostať do vášho zariadenia, poprípade od vás vylákať citlivé údaje či finančné prostriedky.

Nástrahy četovacích aplikácií

Medzi hlavné hrozby, s ktorými sa môžete stretnúť v rámci četovacích aplikácií ako Signal, WhatsApp, Telegram či Facebook Messenger, sú phishingové podvody rôzneho druhu. Najčastejšie sú to správy od neznámych používateľov, ale aj vašich priateľov so skompromitovaným účtom, ktoré vás navádzajú k prejdeniu na škodlivý obsah či odovzdaniu citlivých informácií. Nebezpečné sú aj napodobeniny legitímnych četovacích aplikácií či služby so slabým zabezpečením. Spomenúť však treba aj šírenie hoaxov a dezinformácií.

Ako na bezpečné používanie četovacích aplikácií?

1. Aplikácie udržujte aktualizované.
2. Nastavte súkromie a povolenia podľa svojich preferencií.
3. Používajte aplikácie s end-to-end šifrovaním (napr. Signal a WhatsApp).
4. Aktivujte dvojfaktorové overenie.
5. Sťahujte aplikácie len z oficiálnych zdrojov.
6. Komunikujte iba s osobami, ktoré poznáte.
7. Nezdieľajte súkromné informácie ako heslá alebo finančné údaje.
8. Neklikajte na odkazy od neznámych osôb alebo podozrivé odkazy od priateľov.
9. Nahlasujte nevhodných používateľov a spam.

Nástrahy videoslužieb

Čoraz populárnejším spôsobom komunikácie sú videohovory. Aj keď vidíte osobu na obrazovke, neznamená to, že vám nič nehrozí. Ak voláte s neznámou osobou, môže ísť o útočníka, ktorý si vás nahráva a následne vás môže vydierať zverejnením komunikácie. Čoraz sofistikovanejšie nástroje umelej inteligencie zas umožňujú prostredníctvom technológie deepfake vydávať sa za inú osobu.

Ako na bezpečné používanie videoslužieb?

1. Pri používaní videohovorov v rámci četovacích aplikácií dodržiavajte všetky bezpečnostné zásady platné pre tieto aplikácie spomenuté v príručke.
2. Ak máte externú webovú kameru pripojenú k USB portu vášho počítača, pripojte ju len vtedy, keď ju využívate.
3. Ubezpečte sa, že webovú kameru máte v nastaveniach predvolene vypnutú.
4. Vstavanú webovú kameru prekryte vždy, keď ju nepoužívate.
5. Webové kamery a smart zariadenia s kamerou neumiestňujte na miesta, kde by sa mohli odohrať chúlostivé situácie.
6. Nerobte pred odkrytou webovou kamerou nič, čo by ste normálne nespravili pred očami iných.

Nástrahy e-mailovej komunikácie

E-maily patria aj v súčasnosti k najčastejším spôsobom, akým kyberzločinci útočia na používateľov. Táto forma komunikácie sa vo veľkom zneužíva na rozposielanie phishingových správ imitujúcich rôzne služby (pošta, banka), šírenie škodlivého kódu prostredníctvom odkazov na infikované stránky a prílohy a v neposlednom rade aj na rozosielanie nevyžiadanej pošty – spamu.

Ako používať e-mailovú komunikáciu bezpečne?

1. Keďže e-mailový účet slúži mnohým používateľom na prihlasovanie do ďalších služieb, dajte si obzvlášť záležať na jeho zabezpečení.
2. Uistite sa, že e-mailový účet je chránený silným heslom a dvojfaktorovou autentifikáciou.
3. Používajte bezpečnostný softvér s funkciami Antispam a Anti-Phishing.
4. Dávajte si pozor na e-maily, ktoré prichádzajú od cudzích osôb a vyzývajú vás k urýchlenej akcii.
5. Buďte opatrní pri e-mailoch s prílohami. Väčšinou majú inú príponu ako doc alebo docx, no aj takéto prílohy môžu skrývať škodlivý kód.
6. Zbytočne nezverejňujte vašu e-mailovú adresu.
7. Vytvorte si separátnu e-mailovú adresu na doručovanie propagačných materiálov. Spam tak odkloníte z vašej hlavnej adresy.

Upozornenie: Dávajte si pozor na e-maily prichádzajúce od neznámych osôb, ktoré sa vydávajú za známe osobnosti, amerických vojakov či vzdialených príbuzných v núdzi. Za žiadnych okolností im neposielajte citlivé údaje a financie. Konverzáciu ukončite a kontakt zablokujte.

Sociálne siete

Sociálne siete ako Facebook, Instagram či TikTok sú skvelé miesto na prehlbovanie záujmov či udržiavanie kontaktu so známymi. Aj keď sociálne siete čoraz viac prispievajú k bezpečnosti svojich používateľov, mnohé prípady ohrozenia súkromných údajov vznikajú z nedbanlivosti samotných používateľov. Prílišným zverejňovaním informácií či zlými nastaveniami súkromia nahrávajú do kariet kybernetickým útočníkom.

Nástrahy četovacích aplikácií

Phishing – ide o podvod, ktorý má za cieľ pripraviť vás o citlivé informácie. Častým prípadom je správa, ktorá vyzerá, ako keby vám ju adresovala samotná sociálna sieť. Môže sa v nej písať, že váš účet bol zablokovaný a na jeho odblokovanie je potrebné opätovné prihlásenie. V skutočnosti vás odkáže na falošnú stránku, na ktorej odovzdáte svoje prihlasovacie údaje útočníkom.

Klonovanie profilov – podvodníci odcudzia fotografie, mená a iné špecifické osobné informácie z legitímnych profilov, ktoré sú verejne dostupné, aby vytvorili falošné profily takmer na nerozoznanie od tých skutočných. Po vytvorení falošného profilu sa spravidla podvodníci snažia pridať si priateľov alebo sledovateľov v mene obete. Následne im odosielajú podvodné správy.

Romantické podvody – ich podstata spočíva v tom, že útočníci kontaktujú obete cez falošné profily a predstierajú lásku či záujem o vzťah. Často sa vydávajú napríklad za vojakov alebo boháčov a zameriavajú sa na osamelých ľudí. Keď si získajú náklonnosť obete, požadujú od nej pod rôznymi zámienkami financie. Môžu napríklad predstierať, že sa dostali do núdzovej situácie a potrebujú rýchlo peniaze na lekársku starostlivosť.

Falošné súťaže sú medzi používateľmi veľmi populárne. No existujú prípady, keď za týmito súťažami boli skrytí podvodníci, ktorých cieľom nebolo potešiť používateľov výhrou, ale získať citlivé informácie.

Škodlivý kód sa šíri aj prostredníctvom sociálnych sietí. Môže vaše zariadenie infikovať po tom, ako kliknete na podozrivý odkaz v príspevku alebo v komentári, niekto vám zašle škodlivú prílohu napríklad cez Messenger alebo si stiahnete falošnú aplikáciu sociálnej siete, ktorá sa tvári ako legitímna, no jej jedinou úlohou je šírenie škodlivého kódu alebo získanie vašich údajov.

Čo by ste nemali zverejňovať na sociálnych sieťach?

- Čísla a fotografie osobných dokladov
- Telefónne číslo
- Adresu bydliska a práce
- Poznávaciu značku auta
- Lístky na podujatia s čiarovým alebo QR kódom
- Fotografiu platobnej karty
- Zmluvy, lekárske záznamy a oficiálne dokumenty
- Sexuálny obsah
- Hanlivý a urážlivý obsah
- Dezinformácie
- Fotografie, ktoré vás môžu kompromitovať

Tip: Ak chcete na sociálnej sieti zverejniť fotografiu s vašimi priateľmi alebo blízkymi, dobrým pravidlom je vypýtať si ich súhlas na zverejnenie.

Ako zostať v bezpečí na sociálnych sieťach?

1. Zabezpečte svoje kontá silnými jedinečnými heslami a dvojfaktorovou autentifikáciou.
2. Odhláste sa z účtu, ak ste sa prihlasovali zo zariadenia, ktoré bežne nepoužívate.
3. Vaše účty si nastavte ako súkromné tak, aby zdieľané informácie videli len osoby, ktoré poznáte.
4. Neprijímajte žiadosti o priateľstvo od ľudí, ktorých nepoznáte.
5. Povoľte vaše označovanie na fotografiách až po vašom schválení.
6. Dobre si rozmyslite, čo zverejňujete. Ak sa raz obsah dostane na internet, zostane tam, aj keď ho neskôr stiahnete.

Podvody

Pri väčšine internetových hrozieb nemusia zločinci disponovať pokročilými technickými znalosťami. Najúčinnejšou zbraňou sú podvody, ktoré sa spoliehajú na psychologickú manipuláciu obete. Kým donedávna sa dali často odhaliť pomerne jednoducho pre zlú gramatiku či slabé prepracovanie, s nástupom umelej inteligencie čelia používatelia mimoriadne presvedčivým pokusom.

Phishing

Phishing je forma útoku s využitím metód sociálneho inžinierstva, pri ktorom sa zločinec vydáva za dôveryhodnú osobu alebo inštitúciu s cieľom získať od obete citlivé informácie. Zvyčajne je jeho cieľom zmanipulovať používateľov k vyplneniu dôverných informácií na webových stránkach, ktoré sa na prvý pohľad tvária legitímne. Vo väčšine prípadov sa používa na získanie prístupu k údajom ako:

- čísla bankových účtov,
- čísla bankových kariet,
- heslá PIN,
- používateľské prihlasovacie mená a heslá.

Najčastejšou technikou neoprávneného získavania údajov je vydávať sa za banku alebo finančnú inštitúciu **prostredníctvom falošného e-mailu**, podvodníci vás môžu osloviť aj na sociálnych sieťach. Väčšinou sa snažia presvedčiť obete, že:

- váš účet na sociálnej sieti je v ohrození,
- vaše heslo do online služby bolo prelomené a je potrebné ho zmeniť,
- ste vyhrali v lotérii veľký obnos peňazí,
- vaša banka z bezpečnostných dôvodov zablokovala vašu kartu,
- ste boli obvinený zo závažných trestných činov, pričom sa vydávajú za políciu.

Smishing

Phishing vo forme SMS správy sa nazýva smishing. Často ide o ešte účinnejší druh podvodu ako v prípade online služieb. Čítanosť SMS správ sa blíži k 100 %. Na rozdiel od e-mailov si tak útočníci môžu byť takmer istí, že obeť si prečíta správu.

Mimoriadne nebezpečné je, že prostredníctvom technológie spoofing dokážu zločinci falšovať názov, respektíve telefónne číslo odosielateľa. Správa sa tak môže priradiť ku komunikácii s legitímnym odosielateľom. Podvodná správa teda môže napríklad pôsobiť, že prišla od služby Netflix, doručovacej služby, operátora či banky. Ak správa obsahuje naliehavý tón a skrátený URL odkaz, okamžite zbystrite pozornosť.

Vishing

Útočníci to skúšajú na obete aj prostredníctvom klasických telefonátov. Takejto forme podvodu sa hovorí vishing. Zločinci sa vydávajú za dôveryhodnú osobu či inštitúciu, napríklad zástupcu banky, poskytovateľa IT služieb, pracovníka technickej podpory alebo za vládneho úradníka. V príjemcovi hovoru vytvoria pocit naliehavosti alebo strachu, ktoré prevážia nad jeho prirodzenou opatrnosťou a podozrievavosťou.

Hlasové phishingové útoky sa obvykle vykonávajú pomocou automatických systémov prevodu textu na reč, ktoré obeť nasmerujú k volaniu na číslo ovládané útočníkom. Niekedy sú útoky rovno uskutočnené živým volajúcim. Útočník sa potom snaží pomocou psychologického nátlaku vymámiť z obete informácie potrebné na prevod peňazí.

Znepokojivým fenoménom je technológia deepfake, vďaka ktorej dokážu útočníci pomocou umelej inteligencie meniť hlas volajúceho tak, aby pripomínal niekoho iného. Môže sa tak stať, že vám so žiadosťou o prevod peňazí zavolá osoba, ktorá bude znieť presne ako váš nadriadený. Ak máte akúkoľvek pochybnosť, spojte sa s volajúcim cez iný kanál.

Ako rozpoznáte podvod?

Odhalenie podvodu nemusí byť vôbec jednoduché, kyberzločinci používajú čoraz sofistikovanejšie techniky manipulácie. Naletieť môžu v zhone aj inak obozretní používatelia. Ak si všimnete akýkoľvek z nasledujúcich varovných znakov, zvýšte obozretnosť na najvyššiu úroveň.

Generické oslovenie môže naznačiť, že zločinci skúšajú podvod na mnohých používateľoch.

Žiadosť o osobné údaje indikuje, že niečo nie je v poriadku. Inštitúcie ako banka vás nikdy e-mailom alebo telefonicky neoslovia so žiadosťou o citlivé informácie.

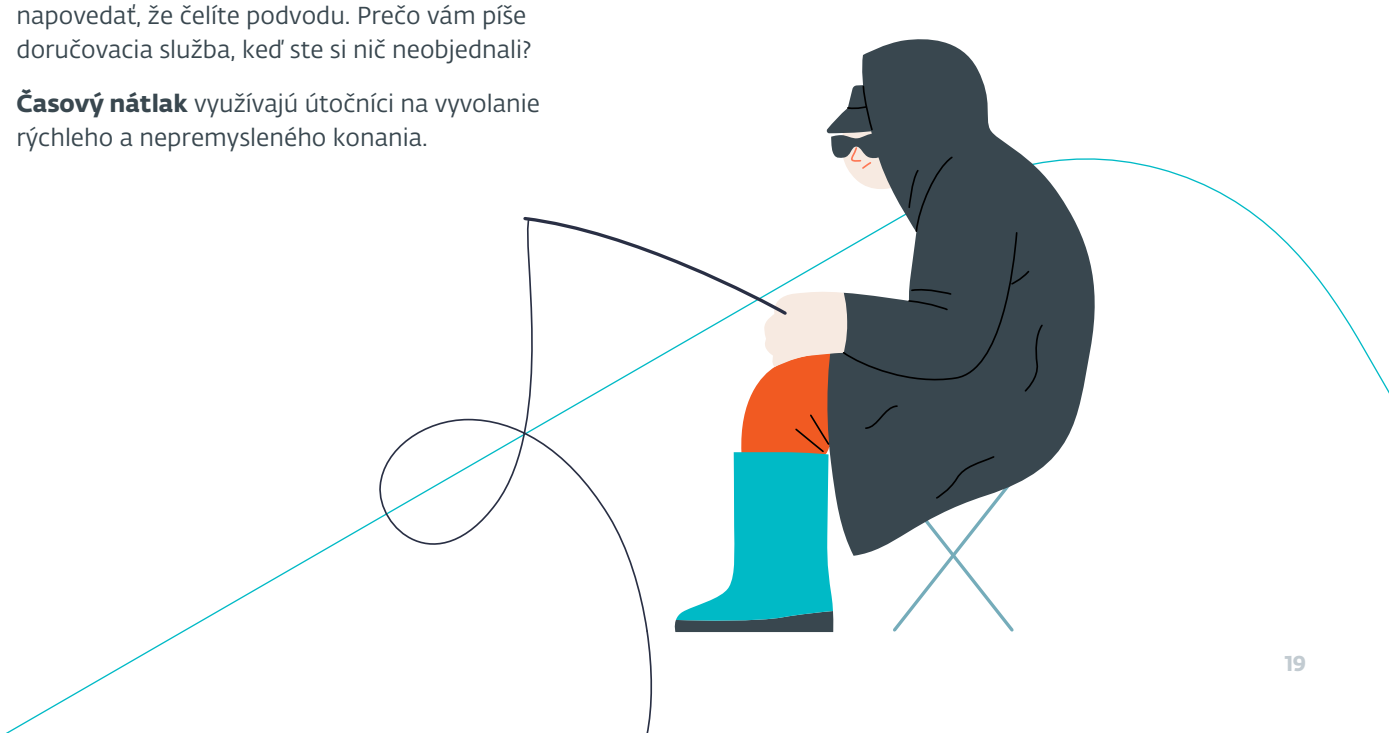
Neočakávaná korešpondencia vám môže napovedať, že čelíte podvodu. Prečo vám píše doručovacia služba, keď ste si nič neobjednali?

Časový nátlak využívajú útočníci na vyvolanie rýchleho a nepremysleného konania.

Príliš lákavá ponuka často slúži ako návnada na krádež peňazí či vylákanie údajov.

Akýkoľvek URL odkaz v neočakávanej či nevyžiadanej správe signalizuje, že sa vás útočníci môžu snažiť dostať k škodlivému obsahu.

Zlá gramatika je v súčasnosti doménou podvodov, na ktorých si útočníci nedali príliš záležať.



Dezinformácie

Dezinformácie aktuálne predstavujú veľké ohrozenie nielen v rámci digitálneho sveta, ale aj celej spoločnosti. Ide o zámerne klamlivé alebo nepravdivé informácie, ktoré majú za cieľ zavádzať ľudí a ovplyvňovať ich názory, postoj alebo konanie. Šíria sa prostredníctvom rôznych kanálov vrátane sociálnych sietí, webových stránok či internetových fór. Môžu ovplyvniť verejné zdravie, politické názory či bezpečnosť krajiny.

Najčastejšie typy dezinformácií

1. **Politické dezinformácie** môžu obsahovať nepravdivé informácie o politikoch, stranách, voľbách a udalostiach, s cieľom ovplyvniť verejnú mienku a náladu voličov.
2. **Medicínske dezinformácie** sa týkajú zdravotníctva a môžu zahŕňať klamstvá o liekoch, vakcínach a pandémiách.
3. **Konšpiračné teórie** tvrdia, že bežné udalosti alebo javy sú zosnované a kontrolované tajnými spoločnosťami, vládami alebo organizáciami.
4. **Náboženské dezinformácie** zahŕňajú šírenie nepravdivých informácií o náboženských textoch, postavách alebo tradíciách.
5. **Ekonomické dezinformácie** šíria falošné informácie o spoločnostiach, ekonomických trendoch alebo investičných príležitostiach.

Niektoré informácie, ktoré sú nepravdivé, nemusia byť primárne vytvorené s úmyslom spôsobiť škodu. Vznikajú nepozornosťou, komunikačným šumom či nesprávnym vyhodnotením informácií. Pre tento druh informácie sa používa termín misinformácia.

Kto a prečo produkuje dezinformácie?

- Mnohé dezinformácie vznikajú ako žart s cieľom zviditeľniť ich autorov.
- Dezinformačné médiá produkujú falošné správy aj s cieľom zisku. Ak majú na stránke umiestnenú reklamu, z kliknutí na správu zarábajú.
- Informácie šíria zámerne rôzne záujmové skupiny. Autori sa usilujú o ovplyvňovanie verejnej mienky, politických postojov alebo volieb, aby dosiahli špecifický cieľ. Niektoré vlády, záujmové skupiny alebo vojenské organizácie môžu používať dezinformácie na získanie výhody v geopolitických súbojoch.

Dezinformačné médiá

Dezinformačné médiá sa často snažia pôsobiť aj po grafickej stránke ako seriózne spravodajské médiá. Vo svojom obsahu preto kombinujú zmes pravdivých správ, pričom iba niektoré články obsahujú klamstvá alebo polopravdy. Ich skutočným cieľom je nenápadne manipulovať recipienta a ovplyvňovať jeho postoje. Takýmto médiám často chýba redakčná štruktúra a postupy. Varovným znakom je aj frekventovaná prítomnosť emočného zafarbenia obsahu.

Internetoví trollovia

Veľkými pomocníkmi dezinformátorov sú internetoví trollovia. Ide o internetové profily, ktoré zámerne šíria konflikty a negatívne emócie medzi ostatnými používateľmi internetu. Ich cieľom je vyvolávať rozbroje a podnecovať kontroverzie. Môže ísť pritom o skutočných ľudí, ktorých povzbudzuje pocit anonymity v online svete, ale aj falošné profily, ktoré majú za úlohu ovplyvniť verejnú mienku.

Ak sa dostanete do situácie, pri ktorej ste svedkami trollingu, mali by ste sa snažiť nezapájať sa do hádok a nereagovať na provokácie. Namiesto toho môžete trolla nahlásiť a upozorniť administrátora platformy.

Ako rozpoznať dezinformácie?

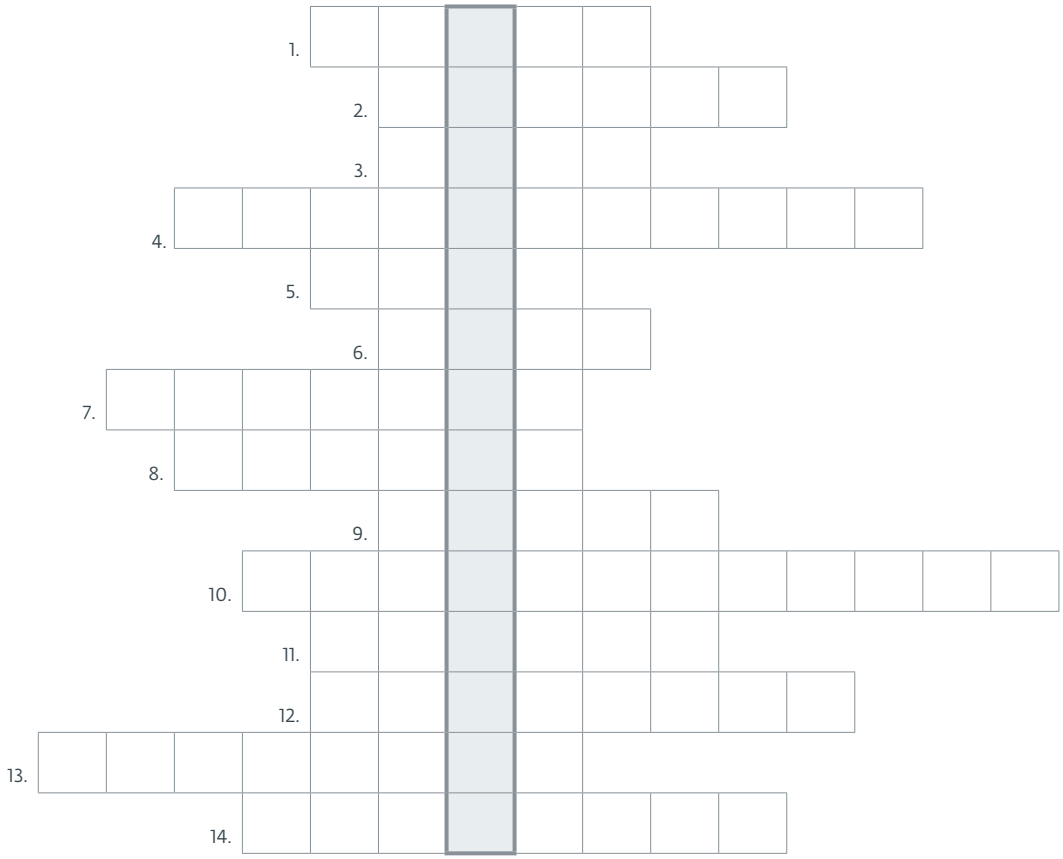
1. **Zdroj informácií** – overte si dôveryhodnosť zdroja – falošné profily a neoverené stránky môžu byť známkou nepravdivých informácií.
2. **Titulky** – bombastické nadpisy môžu zavádzať, preto si prečítajte celý obsah.
3. **Skontrolujte zdroje citácií a štatistík** – ak sa v texte nachádza podozrivý citát alebo štatistika, skontrolujte jej legitímnosť jednoduchým googlením.
4. **Overujte s inými zdrojmi** – hľadajte informáciu, pri ktorej máte pochybnosti, aj v iných médiách.
5. **Obrázky** – skontrolujte, či nie sú upravené alebo nepochádzajú z inej situácie. Použite Google Image Search.
6. **Dátum publikovania** – staré príspevky sa môžu šíriť ako aktuálne, overte si dátum pôvodného zverejnenia.
7. **Hľadajte fakty, nie iba názory** – dôveryhodné zdroje sa zameriavajú na fakty podložené dôkazmi, nie na nepodložené domnienky.
8. **Emocionálne príspevky** – dezinformácie často vzbudzujú silné emócie, buďte skeptickí voči poburujúcim správam.

Tip: Ak narazíte na hoax, ktorý zdieľal váš priateľ, slušne ho na to upozornite. Môžete tak prispieť k zamedzeniu šírenia nepravdivých informácií.

Otestujte si svoje digitálne zručnosti

Kyberkrížovka

Otestujte si svoje znalosti digitálnej bezpečnosti a doplňte chýbajúce slová v tajničke:
_____ _____ môžeme vytvárať bezpečný digitálny svet, v ktorom sú všetky generácie chránené.



1. Tajný kód na prístup k účtom.
2. Škodlivý kód, ktorý sleduje používateľskú aktivitu na zariadeniach.
3. Falošná správa na internete s virálnym dosahom.
4. Zlý kód, ktorý poškodzuje zariadenia.
5. Neoprávnený pokus o prístup k systému.
6. Osobný profil na webovej stránke.
7. Podvod s využitím telefónu.
8. Osoba, ktorá využíva svoje technické znalosti na prístup do počítačových systémov.
9. Prenosné zariadenie na telefonovanie.
10. Slabé miesto v systéme, ktoré môže byť zneužité.
11. Kopírovanie údajov pre ich ochranu v prípade straty.
12. Podvodné pokusy o získanie osobných údajov.
13. Podvod, ktorý sa šíri prostredníctvom SMS správ.
14. Globálna sieť počítačov umožňujúca výmenu informácií a komunikáciu.

Vyhľadajte a zneškodnite škodlivé kódy

V tejto osemsmerovke sa stanete bezpečnostným softvérom, ktorý má za úlohu odhaliť a zneškodniť škodlivé kódy. Stačí nájsť všetky skryté nebezpečné kódy a vymazať ich zo systému, aby ste ochránili online svet.

SPYVÉR
RANSOMVÉR
KEYLOGGER
TRÓJSKY KÔŇ
ADVÉR
ČERV

K	V	R	E	Č	O	A	Ť	F	I
T	R	Ó	J	S	K	Y	K	Ô	Ň
D	R	E	G	G	O	L	Y	E	K
R	Q	S	É	S	T	Q	T	Z	Š
É	L	É	C	Ř	P	U	Ň	F	X
V	U	Á	R	É	V	Y	P	S	Z
D	R	A	N	S	O	M	V	É	R
A	T	H	Ý	Q	H	W	Ó	V	Ó
L	Y	S	B	Ň	Ô	Y	Ľ	Ř	N
T	Ô	Á	A	J	A	É	F	Ň	C

Digitálny kvíz

Otestujte svoje znalosti! Odpovedzte na tri otázky, pričom každá má len jednu správnu odpoveď.

1. Čo je najlepšie urobiť, aby ste zabránili neoprávnenému prístupu k svojim účtom v digitálnych službách?

A. Používať rovnaké heslo pre všetky účty
B. Používať jednoduché heslá, ktoré sa ľahko pamätajú
C. Používať jedinečné a silné heslá pre každý účet

2. Aký je hlavný cieľ phishingového útoku?

A. Zvýšiť návštevnosť webovej stránky
B. Získať citlivé údaje, ako sú heslá, čísla kreditných kariet alebo osobné informácie
C. Propagovať nový produkt alebo službu

3. Aké informácie by ste nemali zdieľať na sociálnych sieťach?

A. Vaše obľúbené filmy a knihy
B. Vašu adresu, telefónne číslo a informácie o vašej platobnej karte
C. Videá

Odpovede

Kyberkrížovka: *1. heslo, 2. spyvér, 3. hoax, 4. škodlivý kód, 5. útok, 6. účet, 7. vishing, 8. hacker, 9. mobil, 10. zraniteľnosť, 11. záloha, 12. phishing, 13. smishing, 14. internet,* Digitálny kvíz: *C, B, B*

BEZPEČNÝ DIGITÁLNY SVET PRE KAŽDÉHO

Vyberte si úroveň ochrany podľa potrieb. Zabezpečte svoje zariadenia antivírusom, blokovaním podvodov aj šifrovaním dát.

Vyše 30

rokov špičkovej kybernetickej ochrany

Vyše 110 miliónov

chránených používateľov na celom svete

Vyše 100

prestížnych ocenení VB100

ESET, spol. s r. o.
Einsteinova 24, 851 01 Bratislava
Slovenská republika
www.eset.sk

Pridajte sa k nám na Facebooku.
http://fb.eset.sk