SociALL

SPRÍSTUPNENIE TECHNOLÓGIÍ V SOCIÁLNEJ STAROSTLIVOSTI PRE VŠETKÝCH

Téma 1.3. Základy online bezpečnosti a kybernetickej bezpečnosti

Financované Európskou úniou. Vyjadrené názory sú len názormi autora (autorov) a nemusia nevyhnutne odrážať názory Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani EACEA za názory nezodpovedajú.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.

MedicalCar

åpenhet

Co-funded by the European Union

Obsah

Úvod do kurzu

1. Základy kybernetickej bezpečnosti a online bezpečnosti
2. Prehľad najčastejších hrozieb
3. Preventívne opatrenia
4. Osvedčené postupy a správne návyky
5. Užitočné nástroje a ďalšie zdroje

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medical car
åpenhet
Co-funded by the European Union

Úvod do kurzu

1. Prehľad kurzu
2. Cieľová skupina
3. Ciele kurzu

Co-funded by the European Union

Úvod do kurzu

1. Prehľad kurzu

O čom je tento kurz?

Kurz „Základy online bezpečnosti a kybernetickej bezpečnosti“ je navrhnutý tak, aby pracovníkom sociálnej starostlivosti poskytol základné vedomosti a zručnosti na **ochranu citlivých údajov a zaistenie online bezpečnosti** v kontexte ich práce. Účastníci sa naučia, ako **identifikovať** a **zmierniť** bežné riziká kybernetickej bezpečnosti a ako prijať **osvedčené postupy** a ľahko implementovateľné opatrenia pre online bezpečnosť.

Prečo na tom záleží?

Nadnárodný výskum projektu SociALL poukázal na: kybernetickú bezpečnosť ako na mimoriadne **dôležitú a aktuálnu** tému v kontexte zvýšeného rizika kybernetickej bezpečnosti, obáv o zdravie a súkromie a integritu osobných údajov. Násobenie kybernetických útokov voči **zraniteľným** organizáciám zdravotných a sociálnych služieb, ako ukázali nedávne vlny ransomvéru na európske nemocnice, si vyžaduje zvýšenú pozornosť a vedomosti.

Co-funded by the European Union

Úvod do kurzu

2. Cieľová skupina

SociALL

Pre koho je kurz určený?

Prakticky **akýkoľvek profesionálny pracujúci v sektore starostlivosti** môže nasledovať tento kurz, krďže každý je pomocou digitálnych nástrojov denne vystavený kybernetickým rizikám. Kurz väčšinou pozostáva z vysvetlení, tipov a osvedčených postupov, ktoré môžu byť pre väčšinu z nich aplikovateľné individuálne a bez dôležitých technických zručností . Väčšina tohto obsahu môže slúžiť pracovníkom v ich profesijnom živote, ale môže sa vzťahovať aj na ich osobné používanie digitálnych nástrojov .

Môžem to nasledovať?

Tento učebný plán je prispôsobený **každému odbornému pracovníkovi** a poskytuje skôr základné, užitočné návody a usmernenia ku kybernetickej bezpečnosti a online bezpečnosti. Každý človek, ktorý je vo svojom profesionálnom živote zvyknutý používať digitálny nástroj, je preto schopný tento kurz sledovať, porozumieť mu a učiť sa z neho.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MedicalScan
åpenhet
Co-funded by the European Union

Úvod do kurzu

3. Ciele kurzu

Čo sa môžem z kurzu naučiť?

- Pochopiť **dôležitosť** kybernetickej bezpečnosti a online bezpečnosti
- Porozumieť **rizikám** a najbežnejším **hrozbám**
- Pochopiť **ľudský faktora** pri kybernetických útokoch
- Uplatňovať **ľahko implementovateľné opatrenia** pre ochranu údajov a online bezpečnosť
- Využívať užitočné **zdroje**, **nástroje** a celosvetovo uznávané **osvedčené postupy** pre zvýšenie bezpečnosti

Čo sa tým zmení?

Na konci školenia budú účastníci a ich organizácia schopní zlepšiť:

- **Online bezpečnosť** vo svojich prevádzkach
- **Identifikovať** a **riešiť riziká** kybernetickej bezpečnosti
- Zmeniť **procesy**, ktoré ich robia **zraniteľnými** voči bezpečnejším procesom
- **Školiť a radiť** svojim kolegom v tejto záležitosti, aby vytvorili **bezpečnejšiu organizačnú kultúru**
- **Odovzdať** tieto poznatky **zraniteľným pacientom/ klientom**, ak ich pracovníci sociálnej starostlivosti vnímajú ako riziko

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

SociALL

1. Školenie: Základy kybernetickej bezpečnosti a online bezpečnosti

1. Dôležitosť kybernetickej bezpečnosti a online bezpečnosti.
2. Pochopenie zodpovednosti pracovníkov starostlivosti za integritu údajov pacientov/klientov.
3. Ľudské chyby a nedbanlivosť sú hlavnými vstupnými dverami pre kybernetickú kriminalitu.
4. Čo môžeme urobiť? Identifikujte a liečte ľudskú zraniteľnosť.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPWA
Medical Car
åpenhet
Co-funded by the European Union

1. Základy kybernetickej bezpečnosti a online bezpečnosti

1.1. Dôležitosť kybernetickej bezpečnosti a online bezpečnosti

Kyberochrana nie je len módne slovo

Je to Štít, ktorý nás chráni pred rôznymi online rizikami vrátane krádeže identity, finančných podvodov, krádeže osobných údajov, kybernetických útokov zneschopňujúci organizáciu ako celok a pod.

Kyberochrana je trojitá ochrana

V sektore starostlivosti je úlohou kybernetickej bezpečnosti chrániť jednotlivých odborných pracovníkov, ich organizácie a ich pacientov/ klientov.

Kybernetické útoky sú novou kriminalitou

Ako ukázala nedávna vlna ransomware útokov na výkupné na zariadenia zdravotnej a sociálnej strarostlivosti (nemocnice, domovy dôchodcov atď.), kybernetické útoky sú čoraz viac nebezpečnejšie a ohrozujú sektor starostlivosti.

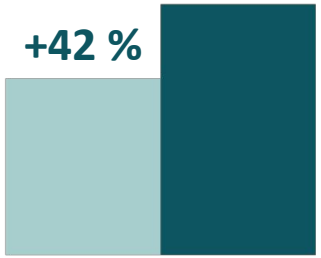
Záver: **Nebezpečenstvo** kyberkriminality nebolo nikdy také existenčné **.** Naša **závislosť** od digitálnych nástrojoch vo všetkých aspektoch života z nás robí **zraniteľné** ciele, pokiaľ nepodnikneme žiadne **kroky** na zaistenie našej digitálnej bezpečnosti.

Co-funded by the European Union

1. Základy kybernetickej bezpečnosti a online bezpečnosti

1.1. Dôležitosť kybernetickej bezpečnosti a online bezpečnosti

Niekoľko údajov z „ Trendy kybernetických útokov: Správa z polovice roka 2022 “ ukazuje, že nebezpečenstvo je skutočné. Len v roku 2022:



Kybernetické útoky na zdravotnícke zariadenia vzrástli o **42 %** v porovnaní s predchádzajúcim obdobím

10 mil. $

Porušenie údajov v sektore zdravotnej starostlivosti znamenalo priemerné celkové náklady **10,10 mil. amerických dolárov** na jeden incident.

1426

Zdravotnícke organizácie **týždenne** zaznamenali **1 426** (zdokumentovaných) **útokov** po celom svete

1/42

1 zo 42 zdravotníckych organizácií sa v treťom štvrťroku 2022 stala obeťou útoku ransomvéru.

Záver: **Nebezpečenstvo** kyberkriminality nebolo nikdy také existenčné**.** Naša **závislosť** od digitálnych nástrojoch vo všetkých aspektoch života z nás robí **zraniteľné** ciele, pokiaľ nepodnikneme žiadne **kroky** na zaistenie našej digitálnej bezpečnosti.

Co-funded by the European Union

1. Základy kybernetickej bezpečnosti a online bezpečnosti

SociALL

1.2. Pochopenie zodpovednosti odborných pracovníkov v starostlivosti za integritu údajov pacientov/ klientov

Dôvera je základným kameňom a základom vzťahu medzi odborným pracovníkom a pacientom/klientom. Ústrednou súčasťou tejto dôvery je schopnosť zodpovedne zaobchádzať s citlivými a osobnými informáciami pacientov/klientov a chrániť ich.

Údaje o pacientoch/klientoch tvoria pokladnicu **osobných** a často **citlivých** informácií.

- História medicíny
- Liečebný plán
- Hygiena Života
- Kontaktné údaje
- Číslo sociálneho poistenia

Profesionálom v oblasti starostlivosti je zverené veľké množstvo **osobných** a **zdravotných** údajov, ktoré môžu zaujímať **rôzne zainteresované strany**, ako sú spoločnosti predávajúce produkty, podvodníkov, ktorí hľadajú ľahké obete, alebo osoby so zlými úmyslami akéhokoľvek druhu.

Čo je dôležitejšie a bez ohľadu na ich hodnotu, tieto údaje sú **osobné** a **súkromné**. Profesionáli v oblasti starostlivosti nesú veľkú zodpovednosť za ich zachovanie a dlhujú to pacientom, ktorí im zverili svoje údaje.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPA
Medicalscan
åpenhet
Co-funded by the European Union

1. Základy kybernetickej bezpečnosti a online bezpečnosti

SociALL

1.2. Pochopenie zodpovednosti odborných pracovníkov v starostlivosti za integritu údajov pacientov/ klientov

Hoci digitálne spracovanie údajov o pacientoch/klientoch uľahčilo život odborným pracovníkom a zvýšilo ich efektivitu, predstavuje zraniteľnosť **a** novú **oblasť ochrany**.

A čo GDPR? HIPAA?

Zákonné povinnosti zabezpečiť minimálnu ochranu a iniciovať pohyb. Odborní pracovníci by však nemali prijímať opatrenia na ochranu údajov len preto, aby dodržiavali tieto povinnosti: ich **etickou povinnosťou je** chrániť **dôstojnosť** a **súkromie** pacientov.

Ochrana údajov presahuje rámec dodržiavania zákonných povinností.

Odborní pracovníci si musia uvedomiť, aký **vplyv môže mať porušenie údajov**, a pochopiť **váhu a dôležitosť** ich **zodpovednosti**. Dôvera ich pacientov závisí od tohto uvedomenia si a rovnako aj morálny záväzok odborných pracovníkov chrániť svojich pacientov/klientov.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPWA
Medicalscan
åpenhet
Co-funded by the European Union

1. Základy kybernetickej bezpečnosti a online bezpečnosti

SociALL

1.3. Ľudské chyby a nedbanlivosť sú hlavnými vstupnými dverami pre kybernetickú kriminalitu

Počítačoví zločinci využívajú **ľudské chyby a nedbalosť.** Tie predstavujú najjednoduchšiu **bránu** a rovnajú sa tomu, ak po opustení zariadenia sociálnych služieb v noci necháte dvere dokorán otvorené, bez dozoru.

Hackovanie softvéru a databáz využívaním ich **technických zraniteľností** existuje, ale je veľmi zriedkavé a predstavuje len malú časť kybernetických útokov. Vo väčšine prípadov počítačoví zločinci jednoducho vojdu dverami, ktoré ľudia ponechali **otvorené – či už v dôsledku chýb alebo nedbanlivosti–, aby získali neoprávnený prístup** a **kompromitovali citlivé informácie**.

„Som opatrovateľka, nie počítačový expert. Prečo by som sa mal starať?"

Takmer pri všetkých kybernetických útokoch, ktorých sa v poslednom čase stalo svedkom sektor starostlivosti (phishing, ransomware atď.), nebol hlavnou príčinou porušenia chybný antivírus, slabý softvér alebo neoptimálna technická architektúra: tieto útoky takmer neustále využívajú **ľudské chyby**, často od samotného odborného personálu.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

1. Základy kybernetickej bezpečnosti a online bezpečnosti

1.4. Čo môžeme urobiť? Identifikujte a liečte ľudskú zraniteľnosť

Kybernetická bezpečnosť v sektore starostlivosti nie je len o individuálnom úsilí – chyba jedného ovplyvňuje všetkých ostatných. Ide o **kolektívnu zodpovednosť**, **informovanosť**, implementáciu **osvedčených postupov** a **školení**.

Kybernetická bezpečnosť je inštitucionálne zložitá otázka, pretože chyba jedného ovplyvňuje všetky (ako napríklad ransomware, ktorého obeťou sa stali mnohé nemocnice). Kvôli tejto všezahrňujúcej povahe je kybernetická bezpečnosť o **zlepšovaní kolektívnej obrany** proti kybernetickým hrozbám, a nie len o zlepšovaní individuálneho správania.

Znamená to **kolektívne úsilie** o **zvýšenie povedomia, zvýšenie zodpovednosti a vlastníctva, vzdelávanie zamestnancov** o kybernetických hrozbách, kolektívne prijatie a uplatňovanie procesov, ktoré integrujú **osvedčené postupy** atď.

Na **individuálnej úrovni** kybernetická bezpečnosť neznamená len rešpektovanie **protokolov** a procesov, ale aj pochopenie postavenia človeka ako **aktéra kybernetickej bezpečnosti inštitúcie**, čo znamená **kritické myslenie a zvyšovanie povedomia** o nebezpečenstvách, príspevok k **školeniam alebo mentoringu** a **aktívne zapojenie** a vlastníctvo.

Co-funded by the European Union

1. Základy kybernetickej bezpečnosti a online bezpečnosti

1.4. Čo môžeme urobiť? Identifikujte a liečte ľudskú zraniteľnosť

Kybernetická bezpečnosť je neistá veda: k narušeniam stále dochádza v dobre chránených a vzdelaných štruktúrach. Organizácie by nemali zanedbávať **nápravné opatrenia a pripravenosť** v prípadoch porušenia.

Dokonca aj so zlepšeným prístupom ku kybernetickej bezpečnosti, lepšími procesmi, vzdelanejším personálom a pod. môže stále dochádzať k narušeniu údajov a kybernetickým útokom, aj keď podstatne menej často. 100 % ochrana neexistuje, a preto je pre zariadenia sociálnej starostlivosti kľúčové, aby mali zavedené kompletné stratégie, ktoré je možné v prípade porušenia bezodkladne zaviesť, a aby boli pripravené na krízový manažment, protiakciu, obnovenie kontroly a zníženie dopadov.

Tieto stratégie by sa však mali skôr rozvíjať na úrovni **technických tímov** a mali by zahŕňať **konkrétnejší technický obsah** . Nápravné opatrenia a pripravenosť ako také nie sú súčasťou tohto učebného plánu, hoci sú absolútne nevyhnutné pre akúkoľvek zariadenie sociálnej starostlivosti.

Co-funded by the European Union

SociALL

2. Školenie: Prehľad najčastejších hrozieb

1. Ochrana pacientov/klientov
2. Phishingové útoky
3. Škodlivý softvér
4. Sociálne inžinierstvo

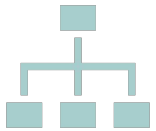
JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MedicalScan
åpenhet
Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.1. Ochrana pacientov/klientov

Online hrozby sa môžu zamerať a poškodiť

Individuálni zamestnanci



Organizácie zdravotnej a sociálnej starostlivosti

Pacienti/ klienti

Najmä určité kategórii pacientov/klientov hrozí väčšie **riziko,** že sa stanú obeťami kybernetických útokov, k tejto kategórii patria napr. **izolovaní starší jednotlivci**.

Odborní pracovníci môžu chrániť svojich pacientov/klientov, keď odhalia online riziká pre ich bezpečnosť týmito spôsobmi

Pozorovať online správanie klientov/pacientov

Diskutovať a pýtať sa na ich online Život

Identifikovať potenciálne riziká v ich online správaní

Upozorniť ich na identifikované

Vzdelávať ich o bezpečnosti

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.

Medical car

åpenhet

Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.2. Phishingové útoky

Phishingové útoky sú **podvodné** pokusy **získať citlivé informácie** vydávaním sa za **dôveryhodné** subjekty.

V sektore starostlivosti môžu mať phishingové útoky väčšinou nasledovnú formu:

Obchodné kompromitujúce podvodné e-maily („lov veľrýb“)

Sofistikované útoky zamerané na **oklamanie** zamestnancov, aby previedli finančné prostriedky alebo odhalili citlivé informácie.

Tieto podvody sa často spúšťajú **e-mailom** na finančnom alebo účtovnom oddelení tým, že **sa vydáva za vedúcich** pracovníkov na vysokej úrovni alebo poverených zamestnancov.

Tieto phishingové e-maily zvyčajne požadujú **naliehavé** platby, zmeny v detailoch dodávateľa alebo citlivé informácie o zamestnancoch, ktoré sú v **hierarchickom vzťahu** medzi odosielateľom a príjemcom.

From: CEO@acmecorp.com
To: Jane@acmecorp.com
Subject: Urgent

I need you to initiate a wire transfer in the sum of $45,250 to the account below. I am boarding a flight and this needs to be done right now. Can you please get this done? Send confirmation of the transfer immediately.

Thanks

Zdroj: Proofpoint

NÁVODY

- ✔ Odosielateľ používa vyššie hierarchické postavenie
- ✔ Pocit naliehavosti – nie je čas na kontrolu / protest
- ✔ Odosielateľ nesmie telefonovať, iba písať
- ✔ Sfalšované meno domény odosielateľa e - mailu

Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.2. Phishingové útoky

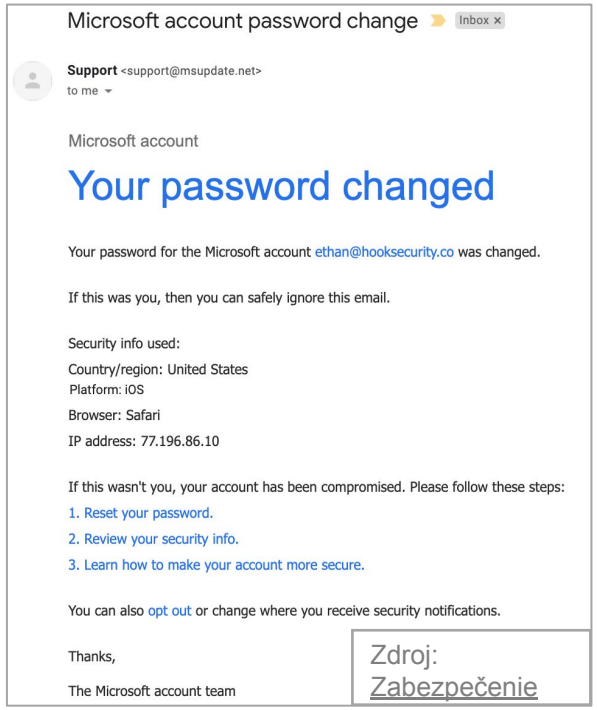
Phishingové útoky sú **podvodné** pokusy **získať citlivé informácie** vydávaním sa za **dôveryhodné** subjekty.

V sektore starostlivosti môžu mať phishingové útoky väčšinou nasledovnú formu:

Phishingové útoky pre získanie poverení

Phishingové útoky pre získanie poverení sa zameriavajú na **krádež** používateľských mien, hesiel a iných prihlasovacích **údajov** s cieľom získať **neoprávnený prístup** k systémom starostlivosti. Tieto podvody často používajú presvedčivé **repliky** legitímnych prihlasovacích stránok, ako sú portály EMR alebo intranetu.

Útočníci posielajú phishingové e-maily alebo nasmerujú obete na **škodlivé webové stránky**, kde zadajú svoje prihlasovacie údaje, **čím nevedomky** poskytnú počítačovým zločincom kľúče k citlivým údajom svojej organizácie.



Microsoft account password change Inbox ×

Support <support@msupdate.net>
to me

Microsoft account

Your password changed

Your password for the Microsoft account ethan@hooksecurity.co was changed.

If this was you, then you can safely ignore this email.

Security info used:
Country/region: United States
Platform: iOS
Browser: Safari
IP address: 77.196.86.10

If this wasn't you, your account has been compromised. Please follow these steps:
1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,
The Microsoft account team

Zdroj: Zabezpečenie

NÁVODY

- ✔ Sfalšovaný názov domény odosielateľa e-mailu (napr. @msupdate.net)
- ✔ Odlišný dizajn e-mailu v porovnaní s bežnými e-mailami spoločnosti
- ✔ Žiadosť o reakciu na niečo, čo ste neurobili (napr. doručenie balíka, ktorý ste si neobjednali).

Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.2. Phishingové útoky

Phishingové útoky sú **podvodné** pokusy **získať citlivé informácie** vydávaním sa za **dôveryhodné** subjekty.

V sektore starostlivosti môžu mať phishingové útoky väčšinou nasledovnú formu:

Phishingové e-maily obsahujúce škodlivý softvér

Phishingové e-maily obsahujúce škodlivý softvér sú navrhnuté tak, aby **oklamali** príjemcov, aby si stiahli a spustili **škodlivý softvér**. Tieto e-maily často obsahujú **infikované prílohy** alebo **odkazy** na napadnuté webové stránky.

Zdravotnícke organizácie sú **obzvlášť zraniteľné** voči malvérovým útokom, pretože úspešné narušenia môžu ohroziť záznamy pacientov, narušiť operácie alebo dokonca ohroziť životy.


Important: Your Password will expire in 1 day(s) Inbox x

MyUniversity 12:18 PM (50 minutes ago)
to me

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Zdroj: Imperva

MY UNIVERSITY

Thank you
MyUniversity Network Security Staff

NÁVODY

- ✔ Pravopisné, gramatické a interpunkčné chyby
- ✔ Odkazy v tele e-mailu, ktoré presmerujú na neočakávané stránky (umiestnením kurzora myši na odkaz zobrazíte adresu URL)
- ✔ Hrozba (napr. zablokovaný účet) alebo pocit naliehavosti
- ✔ Prílohy, ktoré ste si nevyžiadali / nespustili
- ✔ Nezvyčajná žiadosť, tón alebo pozdrav

Co-funded by the European Union

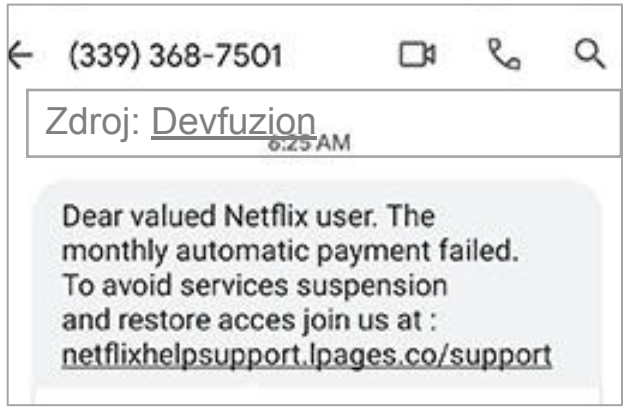
2. Prehľad najčastejších hrozieb

2.2. Phishingové útoky

Phishingové útoky sú **podvodné** pokusy **získať citlivé informácie** vydávaním sa za **dôveryhodné** subjekty. V sektore starostlivosti môžu mať phishingové útoky väčšinou nasledovnú formu:

Vishing a smishing útoky

Vishing (prostredníctvom hlasových správ alebo telefonátov) a **smishing** (prostredníctvom SMS) môže byť realizovaný ktorýkoľvek z predchádzajúcich phishingových útokov. Jednoducho nahradia klasický e-mail iným komunikačným prostriedkom (SMS, volanie atď.).



NÁVODY

Vishing

- ✔ Urgentný tón: podvodníci využívajú strach alebo paniku
- ✔ Žiadosť o dôverné alebo osobné informácie
- ✔ Predstieraný volajúci: väčšina organizácií, ktoré podvodníci predstierajú, že ich zastupujú, bežne netelefonujú zákazníkom.

Smishing

- ✔ Neznáme číslo, nie je uvedené na internete
- ✔ Navštívte webovú stránku predstieraného odosielateľa – napr.: banky na svojich stránkach píšu, že neposielajú SMS
- ✔ Kontaktujte priamo zákaznícky servis spoločnosti

Co-funded by the European Union

2. Prehľad najčastejších hrozieb

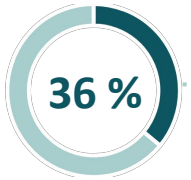
2.2. Phishingové útoky

Phishingové útoky sú **podvodné** pokusy **získať citlivé informácie** vydávaním sa za **dôveryhodné** subjekty.

Niekoľko údajov z **roku 2022** ukazuje, aký rozšírený, sofistikovaný a nebezpečný je phishing (Zdroj: Stationx.net)

3,4 B

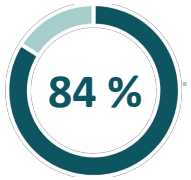
Phishing je najbežnejšou **formou počítačovej kriminality**. Odhaduje sa, že **3,4 miliardy e-mailov denne** sú phishingové útoky odoslané počítačovými zločincami. Je to viac ako **bilión** phishingových e-mailov **ročne** .



36 % všetkých porušení údajov zahŕňa phishing.

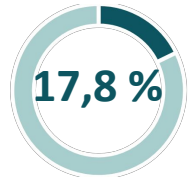
Odcudzenie identity e-mailov predstavuje odhadom **1,2 % celkovej e-mailovej prevádzky** na celom svete.

1,2 %



84 % organizácií bolo v roku 2022 cieľom aspoň **jedného pokusu o phishing.**

Priemerná miera kliknutí na phishingovú kampaň je **17,8 %.**



3 %

V priemere 3 % zamestnancov klikne na škodlivý odkaz v rámci phishingového e-mailu.

Co-funded by the European Union

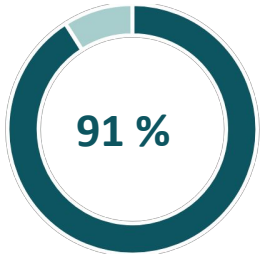
2. Prehľad najčastejších hrozieb

2.2. Phishingové útoky

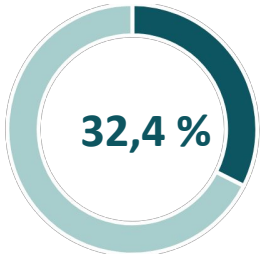
Phishingové útoky sú **podvodné** pokusy **získať citlivé informácie** vydávaním sa za **dôveryhodné** subjekty.

Niekoľko údajov z **roku 2022** ukazuje, aký rozšírený, sofistikovaný a nebezpečný je phishing (Zdroj: Stationx.net

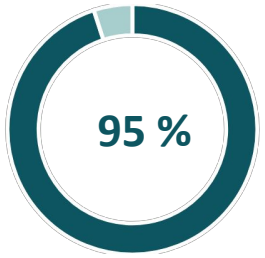
)



všetkých kybernetických útokov sa začína phishingovým **e-mailom**

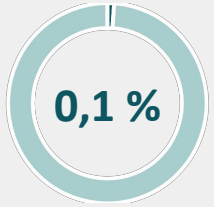


nevyškolených zamestnancov **môžu** napadnúť phishingové podvody

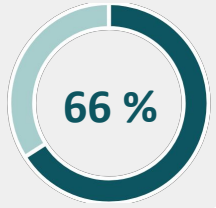


úspešných porušení sú priamo spôsobené **ľudskou chybou**

malé organizácie majú o **350 %** vyššiu pravdepodobnosť, že sa stanú **terčom** phishingu, než väčšie organizácie



0,1 % zo všetkých e-mailových phishingových útokov je zodpovedných za **66 %** všetkých porušení
(zvyčajne cielené, personalizované „spear-phishing“ útoky)



Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.3. Škodlivý softvér

Škodlivý softvér je zastrešujúci pojem zahŕňajúci rôzne typy škodlivého softvéru určeného na narušenie, poškodenie alebo získanie prístupu k počítačovým systémom, sieťam alebo zariadeniam. V sektore starostlivosti má malvér väčšinou podobu:

Vírusy

Vírusy sú škodlivé programy, ktoré **infikujú** iné súbory alebo softvér v počítači a replikujú sa pri **spustení infikovaných súborov**. Môžu spôsobiť poškodenie údajov, softvéru a hardvérových komponentov.

Napríklad phishingové e-maily alebo SMS obsahujúce škodlivý softvér môžu používateľov oklamať, aby klikli na **odkazy** alebo stiahli infikované **súbory.** Tieto infikované súbory alebo odkazy budú „aktivované“ až po kliknutí používateľa, preto je potrebné byť opatrný pri prijímaní nevyžiadaných e-mailov.

POZOR

Mnohé podvody využívajú váš **strach z vírusov** na to, aby vás nakazili: ak vyskakovacia správa antivírusu, ktorý nemáte, signalizuje potenciálnu infekciu vášho zariadenia a ponúka riešenie kliknutím na tlačidlo alebo zavolaním na číslo, nereagujte, veľmi dobre to môže viesť k spusteniu vírusu.

Zdroj: komunita Microsoft

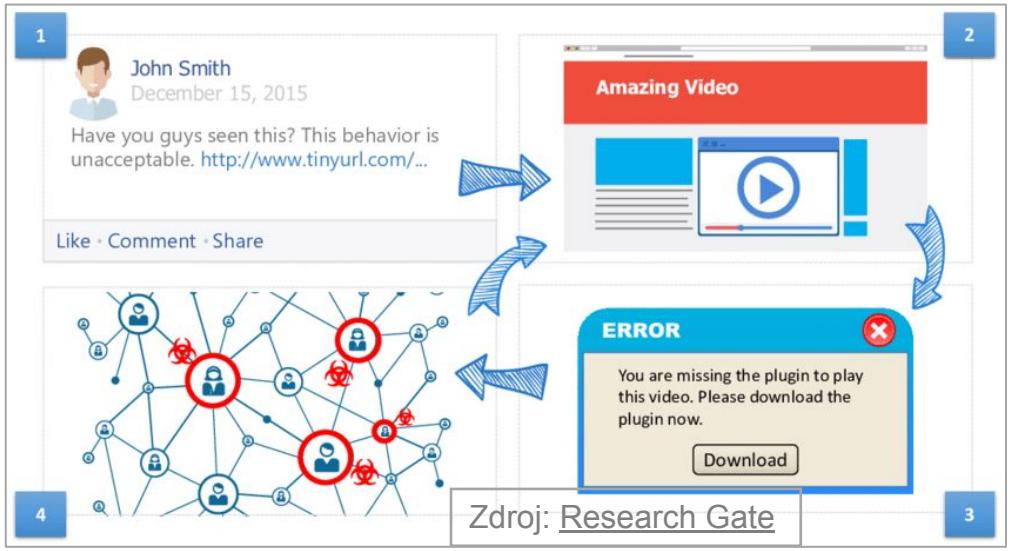
2. Prehľad najčastejších hrozieb

2.3. Škodlivý softvér

Škodlivý softvér je zastrešujúci pojem zahŕňajúci rôzne typy škodlivého softvéru určeného na narušenie, poškodenie alebo získanie prístupu k počítačovým systémom, sieťam alebo zariadeniam. V sektore starostlivosti má malvér väčšinou podobu:

Trójske kone

Trójske kone alebo trójske kone sú malvéry, **ktorý sa vydáva za legitímny softvér**. Oklamú používateľov, aby si ich nainštalovali, často tak, že sa javia ako neškodné súbory alebo aplikácie. Po nainštalovaní môžu trójske kone vykonávať rôzne škodlivé činnosti, ako napríklad kradnúť citlivé údaje, upravovať informácie alebo poskytovať neoprávnený prístup útočníkom. Trójske kone sú často spúšťané phishingovými e-mailami alebo správami.



Zdroj: Research Gate

NÁVODY

- ✔ Počítač beží pomalšie ako zvyčajne.
- ✔ Na zariadení sa zobrazujú neautorizované aplikácie.
- ✔ Časté pády a zamŕzanie zariadenia.
- ✔ Časté vyskakovacie okná.
- ✔ Niektoré aplikácie sa nespustia.
- ✔ Časté prerušovanie internetového pripojenia.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MedicalScan
åpenhet
Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.3. Škodlivý softvér

Škodlivý softvér je zastrešujúci pojem zahŕňajúci rôzne typy škodlivého softvéru určeného na narušenie, poškodenie alebo získanie prístupu k počítačovým systémom, sieťam alebo zariadeniam. V sektore starostlivosti má malvér väčšinou podobu:

Ransomwares

Ransomvér je typ škodlivého softvéru, ktorý šifruje súbory v počítači alebo zariadení obete, čím ich **zneprístupní, kým nebude zaplatené výkupné**. Ransomvérové útoky zvyčajne vyžadujú platbu v kryptomene a môžu spôsobiť značné finančné straty a straty údajov.

Nemocnice a zdravotnícke zariadenia, ktorých systémy sú životne dôležité pre ich fungovanie, boli čiastočne zasiahnuté. V roku 2022 bolo **66 %** nemocníc v USA **cieľom** (nie vždy obeťou) ransomvérového útoku. Organizácie v sektore zdravotníctva **zaplatili** výkupné v približne **61 %** prípadov ransomvéru v roku 2022.

Zdroj: Healthcare IT News

2. Prehľad najčastejších hrozieb

2.3. Škodlivý softvér

Škodlivý softvér je zastrešujúci pojem zahŕňajúci rôzne typy škodlivého softvéru určeného na narušenie, poškodenie alebo získanie prístupu k počítačovým systémom, sieťam alebo zariadeniam. V sektore starostlivosti má malvér väčšinou podobu:

Worms

Červy sú samostatné malvérové programy, ktoré sa **replikujú** v sieťach a zvyčajne využívajú zraniteľné miesta v operačných systémoch alebo sieťových protokoloch.

Môžu sa rýchlo šíriť a spôsobiť **preťaženie siete** alebo vykonávať iné škodlivé činnosti.

Spywares

Spywares sú navrhnuté tak, aby **tajne monitorovali** a zhromažďovali informácie o aktivitách používateľa na jeho počítači alebo zariadení.

Môžu **sledovať stlačenie klávesov, zachytávať snímky obrazovky, zaznamenávať zvyky prehliadania** a kradnúť **citlivé informácie**, ako sú heslá a finančné údaje.

Addwares

Adwarres sú nechcené softvéry, ktoré zobrazujú **reklamy**, často vo forme kontextových reklám alebo presmerovaní prehliadača.

Hoci adware nie je vo svojej podstate škodlivý, môže **znížiť výkon systému**, ohroziť **súkromie používateľov** a viesť k **ďalším infekciám**, ak sa neodstráni.

Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.3. Škodlivý softvér

Škodlivý softvér je zastrešujúci pojem zahŕňajúci rôzne typy škodlivého softvéru určeného na narušenie, poškodenie alebo získanie prístupu k počítačovým systémom, sieťam alebo zariadeniam. V sektore starostlivosti má malvér väčšinou podobu:

Keyloggery

Keyloggery sú typom spywaru, ktorý zaznamenáva **stlačenia klávesov** zadaných používateľom a zachytáva citlivé informácie, ako sú **heslá** , **používateľské mená** a podrobnosti o **kreditných kartách** .

Útočníci môžu pomocou keyloggerov ukradnúť osobné informácie a spáchať krádež identity.

Botnety

Botnety sú **siete napadnutých počítačov** alebo zariadení kontrolovaných útočníkmi.

Botnety môžu byť použité na vykonávanie distribuovaných útokov **typu denial-of-service (DDoS)**, odosielanie **spamových e-mailov** alebo vykonávanie iných škodlivých aktivít **bez vedomia vlastníkov**.

Backdoors

Zadné vrátka sú **skryté vstupné body** alebo zraniteľné miesta úmyselne vytvorené útočníkmi v softvéri alebo systémoch, čo umožňuje **neoprávnený prístup pre budúce zneužitie alebo kontrolu**.

Tieto zadné vrátka umožňujú útočníkom **tajne a na diaľku** prevziať kontrolu nad zariadením, inštalovať ďalší malvér, zaznamenávať stlačenia klávesov atď.

Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.3. Škodlivý softvér

Tieto rôzne typy malvéru sú často kombinované v rámci jedného programu alebo súboru.

Niekoľko údajov z **roku 2022** ukazuje, aké rozšírené, sofistikované a nebezpečné sú malvéry (Zdroj: Getastra.com)

1 bilión

Denne sa zistí **560 000 nových kusov škodlivého softvéru** . V súčasnosti existuje viac ako **1 miliarda škodlivých programov.**

4,5 milióna dolárov

Každú minútu sa **4 spoločnosti** stanú obeťou ransomvérových útokov. **Sektor starostlivosti** je najviac cielený a ten, ktorý platí výkupné najviac. Priemerné náklady na ransomvérový útok sú **4,54 miliónov dolárov.**

50 %

V prípade ransomvérových incidentov sa len **50 %** organizácií, ktoré zaplatili výkupné, **podarilo** získať **svoje údaje späť**. **64 %** organizácií, na ktoré sa zamerali útoky ransomvéru, boli skutočne **infikované**.

+87 %

Za posledné desaťročie došlo **k 87 % nárastu** infikovania škodlivým softvérom. **Trójske kone** tvoria **58 %** všetkého počítačového malvéru. Odhaduje sa, že náklady na počítačovú kriminalitu **v roku 2023** dosiahnu 8 biliónov dolárov.

Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.4. Sociálne inžinierstvo

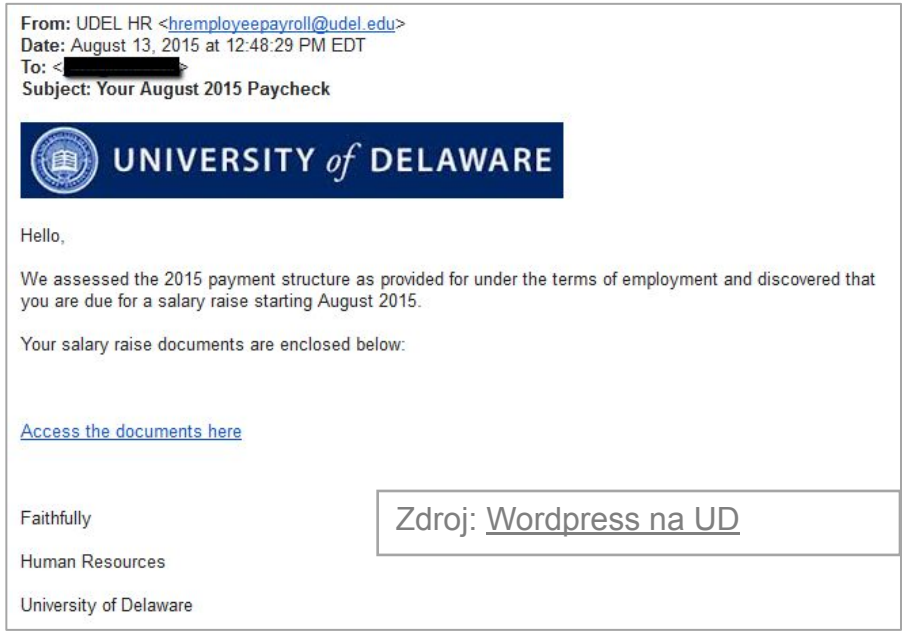
Sociálne inžinierstvo sa vzťahuje na používanie sociálnej taktiky na využitie dôvery, nedbalosti alebo nevedomosti zamestnancov na získanie dôverných informácií. Zatiaľ čo phishingové a malvérové útoky často využívajú tieto zraniteľnosti a **prekrývajú sa** so sociálnym inžinierstvom, čisté sociálne inžinierstvo priamejšie využíva **sociálne taktiky** a môže zahŕňať:

Spear phishing

Spear phishing je **cielená forma phishingu**, ktorá **prispôsobuje útok** konkrétnym jednotlivcom alebo organizáciám.

Útočníci zhromažďujú informácie o svojich cieľoch zo sociálnych médií, verejných databáz alebo predchádzajúcich interakcií, aby si prispôsobili phishingové e-maily a zvýšili pravdepodobnosť úspechu.

Spear phishing správy môžu obsahovať malvér rôzneho typu, môžu priamo požadovať osobné údaje (napr. telefónne číslo na vyriešenie „naliehavej záležitosti“), žiadať o zaplatenie faktúry atď.


From: UDEL HR <hremployeepayroll@udel.edu>
Date: August 13, 2015 at 12:48:29 PM EDT
To: <[redacted]>
Subject: Your August 2015 Paycheck

UNIVERSITY of DELAWARE

Hello,

We assessed the 2015 payment structure as provided for under the terms of employment and discovered that you are due for a salary raise starting August 2015.

Your salary raise documents are enclosed below:

Access the documents here

Faithfully

Human Resources

University of Delaware

Zdroj: Wordpress na UD

2. Prehľad najčastejších hrozieb

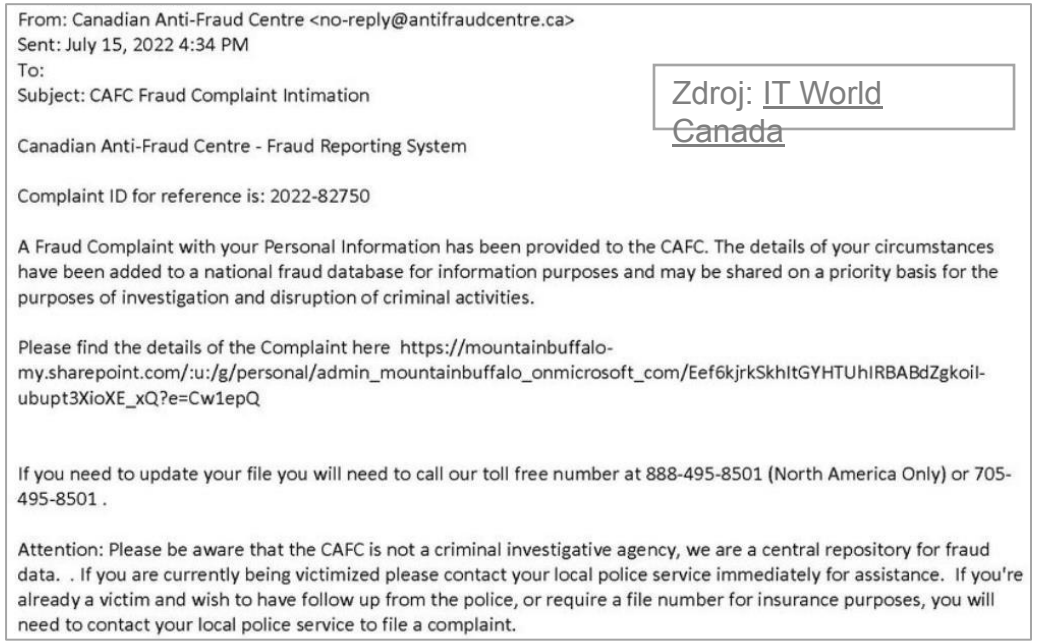
2.4. Sociálne inžinierstvo

Sociálne inžinierstvo sa vzťahuje na používanie sociálnej taktiky na využitie dôvery, nedbalosti alebo nevedomosti zamestnancov na získanie dôverných informácií. Zatiaľ čo phishingové a malvérové útoky často využívajú tieto zraniteľnosti a **prekrývajú sa** so sociálnym inžinierstvom, čisté sociálne inžinierstvo priamejšie využíva **sociálne taktiky** a môže zahŕňať:

Pretextovanie

Pretextovanie zahŕňa vytvorenie **vymysleného scenára alebo zámienky** na manipuláciu jednotlivcov, aby prezradili dôverné informácie alebo vykonali konkrétne akcie.

Útočníci sa často vydávajú za **dôveryhodné subjekty** , ako sú pracovníci IT podpory, policajti alebo vedúci pracovníci spoločností, aby získali dôveru cieľa a získali citlivé informácie. Podvody so zámienkou môžu mať veľmi podobné výsledky ako akýkoľvek typ phishingového podvodu, vyžiadanie platby, krádež poverení alebo osobných údajov atď.



From: Canadian Anti-Fraud Centre <no-reply@antifraudcentre.ca>
Sent: July 15, 2022 4:34 PM
To:
Subject: CAFC Fraud Complaint Intimation

Canadian Anti-Fraud Centre - Fraud Reporting System

Complaint ID for reference is: 2022-82750

A Fraud Complaint with your Personal Information has been provided to the CAFC. The details of your circumstances have been added to a national fraud database for information purposes and may be shared on a priority basis for the purposes of investigation and disruption of criminal activities.

Please find the details of the Complaint here https://mountainbuffalo-my.sharepoint.com/:u:/g/personal/admin_mountainbuffalo_onmicrosoft_com/Eef6kjrkSkhItGYHTUhIRBABdZgkoil-ubupt3XioXE_xQ?e=Cw1epQ

If you need to update your file you will need to call our toll free number at 888-495-8501 (North America Only) or 705-495-8501 .

Attention: Please be aware that the CAFC is not a criminal investigative agency, we are a central repository for fraud data. . If you are currently being victimized please contact your local police service immediately for assistance. If you're already a victim and wish to have follow up from the police, or require a file number for insurance purposes, you will need to contact your local police service to file a complaint.

Zdroj: IT World Canada

Co-funded by the European Union

2. Prehľad najčastejších hrozieb

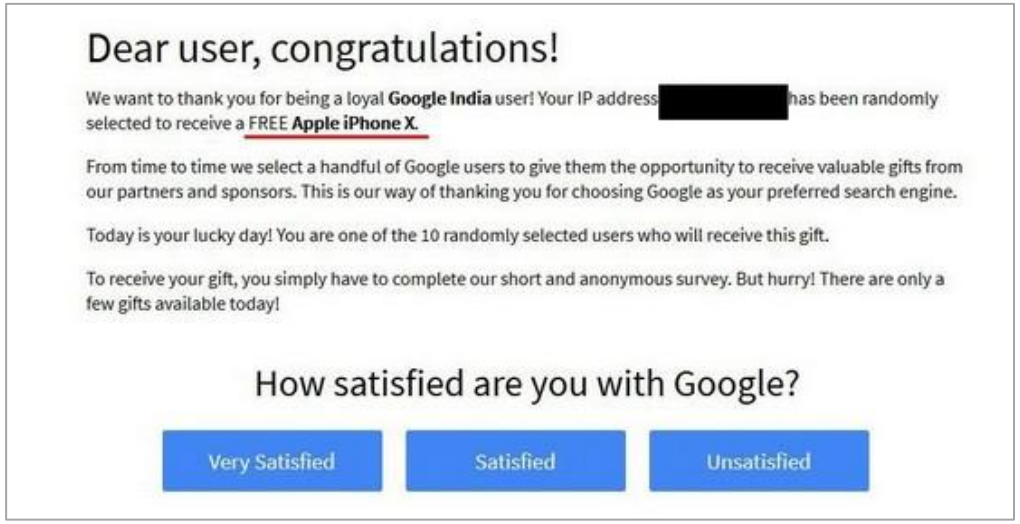
2.4. Sociálne inžinierstvo

Sociálne inžinierstvo sa vzťahuje na používanie sociálnej taktiky na využitie dôvery, nedbalosti alebo nevedomosti zamestnancov na získanie dôverných informácií. Zatiaľ čo phishingové a malvérové útoky často využívajú tieto zraniteľnosti a **prekrývajú sa** so sociálnym inžinierstvom, čisté sociálne inžinierstvo priamejšie využíva **sociálne taktiky** a môže zahŕňať:

Návnady

Návnady sa spoliehajú na **zvedavosť alebo chamtivosť** jednotlivcov, aby ich nalákali na stiahnutie škodlivých súborov alebo návštevu napadnutých webových stránok. Útočníci ponúkajú **lákavé návnady** , ako je napríklad sťahovanie bezplatného softvéru, sťahovanie filmov alebo darčekové karty, ktoré obsahujú malvér alebo pri prístupe vedú k phishingovým stránkam.

Zraniteľné miesta používateľa a zvýšiť **dôveryhodnosť** odosielateľa.



Zdroj: Dummies.com

2. Prehľad najčastejších hrozieb

2.4. Sociálne inžinierstvo

Sociálne inžinierstvo sa vzťahuje na používanie sociálnej taktiky na využitie dôvery, nedbalosti alebo nevedomosti zamestnancov na získanie dôverných informácií. Zatiaľ čo phishingové a malvérové útoky často využívajú tieto zraniteľnosti a **prekrývajú sa** so sociálnym inžinierstvom, čisté sociálne inžinierstvo priamejšie využíva **sociálne taktiky** a môže zahŕňať:

Tailgating (Pripútanie):

Tailgating alebo privinutie zahŕňa **fyzické získanie neoprávneného prístupu** do obmedzených oblastí alebo systémov sledovaním oprávnenej osoby.

Útočníci využívajú **ľudskú zdvorilosť alebo nedostatok vedomia** na to, aby vstúpili do bezpečných priestorov bez riadneho povolenia.

Útoky na napájadlo

Útoky na zalievanie sa zameriavajú na konkrétne skupiny alebo organizácie infikovaním **webových stránok navštevovaných ich členmi** škodlivým softvérom.

Útočníci kompromitujú legitímne webové stránky, aby **šírili škodlivý softvér** nič netušiacim návštevníkom, pričom zneužívajú ich dôveru v napadnutú stránku.

Odcudzenie identity (krádež identity):

Väčšina phishingových taktík zahŕňa určitú formu odcudzenia identity. Niektoré však obsahujú ďalšie prvky na zvýšenie dôveryhodnosti, ktoré predstavujú **krádež identity** .

Môžu zahŕňať ukradnuté alebo sfalšované poverenia a dokumenty, prvky vytvorené IA atď. s cieľom **oklamať** ich pravosť.

Co-funded by the European Union

2. Prehľad najčastejších hrozieb

2.4. Sociálne inžinierstvo

Sociálne inžinierstvo často predstavuje bránu na doručenie škodlivého softvéru alebo prinútenie obetí vykonať akciu.

Niekoľko čísel z **roku 2023** ukazuje, aké rozšírené, sofistikované a nebezpečné je sociálne inžinierstvo (Zdroj: Resmo)

90 %

90 % porušení údajov a **98 %** kybernetických útokov (úspešných alebo neúspešných) malo prvky sociálneho inžinierstva.

4,5 milióna dolárov

Porušenia údajov iniciované technikami sociálneho inžinierstva **stáli v priemere viac ako 4,5 milióna dolárov**.

700

Typická organizácia (v USA) bola ročne terčom viac ako **700 útokov sociálneho inžinierstva.**

+ 354 %

Útoky na prevzatie účtov vzrástli v roku 2023 medziročne o 354 %.

Co-funded by the European Union

SociALL

3. Preventívne opatrenia

1. Zabezpečenie hesla
2. Dvojfaktorové overenie (2FA)
3. Antivírus
4. Aktualizácie softvéru
5. Zabezpečenie
6. Zálohovanie dát

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscar
åpenhet
Co-funded by the European Union

3. Preventívne opatrenia

3.1. Zabezpečenie heslom

Prečo je to dôležité ?

Zabezpečenie hesla je **prvou slabinou** , ktorú využívajú počítačoví zločinci. **Silnejšie** heslá (tj komplikovanejšie a rôznorodejšie) je ťažšie uhádnuť alebo odhaliť pomocou útokov hrubou silou, a preto môžu byť adoptovanou a užitočnou **prvou líniou obrany** proti kybernetickým útokom.

Čo môžem urobiť ?

- Nastavte **silné** heslá: aspoň **16** znakov s veľkými a malými písmenami, číslami a špeciálnymi znakmi.
- **Transformujte vety** na heslá a nie na slová pomocou kódu na transformáciu rôznych typov písmen. Príklad: „Icàre@b0utSecur1ty!“
- Používajte **správcov hesiel** , ktorí si za vás pamätajú vaše heslá a generujú heslá.

Čo môže moja organizácia urobiť?

- Nakonfigurujte svoje systémy (e-mail, online nástroje na odosielanie správ, ERP, CRM atď.), aby ste prinútili používateľov **pravidelne si obnovovať svoje heslo.** Tým sa skráti čas, počas ktorého zostane dané heslo platné.
- Nakonfigurujte **pravidlá hesiel**, aby ste zaistili, že používatelia nebudú používať **rovnaké heslo dvakrát** a že heslo bude **dostatočne silné**.
- Vynútiť všeobecné **obnovenie hesla** po porušení.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

3. Preventívne opatrenia

3.1. Zabezpečenie heslom

Prečo je to dôležité ?

Zabezpečenie hesla je **prvou slabinou**, ktorú využívajú počítačoví zločinci. **Silnejšie** heslá (tj. komplikovanejšie a rôznorodejšie) je ťažšie uhádnuť alebo odhaliť pomocou útokov hrubou silou, a preto môžu byť adoptovanou a užitočnou **prvou líniou obrany** proti kybernetickým útokom.

ZOOM na správcov hesiel

- Správcovia hesiel **uchovávajú vaše heslá** a oslobodzujú vás od povinnosti pamätať si ich. Ako cloudové riešenia zostávajú **dostupné z iných zariadení** .
- Registrácia hesla môže byť vykonaná **manuálne** alebo **automaticky .** Môžete tiež nastaviť správcu hesiel tak, aby pri pripájaní k vašim účtom automaticky vypĺňal pole pre heslo.
- Lepšie je, že správcovia hesiel môžu **generovať jedinečné, veľmi silné heslá** pre každý z vašich účtov a pamätať si ich za vás. Ani ich nemusíte poznať.
- Jediné, čo si musíte zapamätať, je **jedno veľmi silné heslo** – to, ktoré vám dáva prístup k správcovi hesiel.

Užitočné nástroje

- Dashlane
- 1Heslo
- LastPass
- Bitwarden

Co-funded by the European Union

3. Preventívne opatrenia

3.2. Dvojfaktorové overenie (2FA)

Prečo je to dôležité ?

2FA drasticky zlepšuje bezpečnosť: táto metóda overenia vyžaduje použitie aspoň **dvoch zariadení** na prihlásenie do účtu, pričom obe musia byť vopred **zaregistrované** a **dôveryhodné.** Táto metóda nielenže poskytuje používateľovi **kontrolu** nad účtom, ktorý mohol byť napadnutý, ale môže tiež **naznačovať**, že sa tak stalo.

Čo môžem urobiť ?

- **Povoľte 2FA** čo najskôr – to bude byť tiež neskoro raz heslo alebo účet je kompromitovaný .
- Vo väčšine softvéru a webových stránok ste bude nájsť schopnosť to povoliť _ pod **Nastavenia > Zabezpečenie** (IOS a Microsoft, služby Google, sociálne médiá atď.)
- Najpoužívanejším a najspoľahlivejším spôsobom je použitie **dvoch zariadení** patriacich používateľovi (napr. telefón a počítač) zaregistrovaných na účte.

Čo môže moja organizácia urobiť?

- Pre väčšinu systémov môže vaše IT oddelenie presadiť **2FA v celom systéme** pre všetkých používateľov. 2FA sa môže označovať aj ako „ dvojstupňové overenie“ alebo „viacfaktorové overenie“.
- To si však vyžaduje, aby všetci **zamestnanci mali prístup k 2 zariadeniam** , ideálne len na profesionálne použitie, čo nemusí byť tento prípad. Alternatívne môžu byť zamestnanci **vyzvaní**, aby povolili 2FA.

Co-funded by the European Union

3. Preventívne opatrenia

3.2. Dvojfaktorové overenie (2FA)

Prečo je to dôležité ?

2FA drasticky zlepšuje bezpečnosť: táto metóda overenia vyžaduje použitie aspoň **dvoch zariadení** na prihlásenie do účtu, pričom obe musia byť vopred **zaregistrované** a **dôveryhodné.** Táto metóda nielenže poskytuje používateľovi **kontrolu** nad účtom, ktorý mohol byť napadnutý, ale môže tiež **naznačovať**, že sa tak stalo.

Ako to spravím?

- Google Workspace (Gmail, Gdrive , Kalendár atď.)
- Microsoft 365 (Outlook, OneDrive, Teams atď.)
- Slack
- Zoom

A iní - všeobecne dostupné v **bezpečnostnej relácii Nastavenia** pre väčšinu digitálnych nástrojov – aj na osobné použitie (sociálne médiá, bankovníctvo , elektronický obchod, vládne aplikácie a webové stránky atď.).

Co-funded by the European Union

3. Preventívne opatrenia

3.3. Antivírus

Prečo je to dôležité ?

Antivírus chráni svojho vlastníka **skenovaním potenciálnych hrozieb a zisťovaním rizík** , od e-mailového phishingu alebo pokusov o malvér až po podvodné webové stránky a programy. Táto ochrana sa vzťahuje aj mimo počítača na akékoľvek **externé zariadenia**, ktoré s ním interagujú, ako sú napríklad USB kľúče, ktoré môžu prenášať aj malvér.

Čo môžem urobiť?

- **Autonómne nainštalujte** antivírusový softvér, ak ho neposkytuje vaša organizácia (alebo **obhajujte**, aby sa to robilo v rámci celej organizácie). Nechránené počítače sú **ľahkým cieľom** kyberzločincov.
- Pamätajte, že antivírusy sú ďalšou vrstvou zabezpečenia**, ktorá stále závisí od ľudského** faktora: zachovajte **rovnakú úroveň ostražitosti** online bez ohľadu na to, či ste „chránení“ alebo nie.

Čo môže moja organizácia urobiť?

Vaše IT oddelenie môže a **malo by** inštalovať, konfigurovať a spravovať aktualizácie celosystémového **antivírusového softvéru**, aby sa zabezpečila lepšia ochrana digitálnej bezpečnosti organizácie.

Užitočné nástroje

ESET
Kaspersky
Bitdefender
AVG

Co-funded by the European Union

3. Preventívne opatrenia

3.4. Aktualizácie softvéru

Prečo je to dôležité ?

Udržiavanie softvéru a operačných systémov **v aktuálnom stave** bráni počítačovým zločincom vo využívaní známych **bezpečnostných problémov** : poskytovatelia softvéru pravidelne záťažovo testujú svoju vlastnú bezpečnosť. Keď zistia potenciálne narušenia bezpečnosti, **vydajú aktualizácie**, ktoré odstránia tieto zraniteľnosti alebo ich urobia nevyužiteľnými.

Čo môžem urobiť ?

Keď dostanete upozornenie na aktualizáciu, neodkladajte aktualizáciu všetkého softvéru a aplikácií, ktoré používate (osobne aj profesionálne). Pravidelne overujte, či je všetko aktuálne vo vašom aplikačnom centre.

Čo môže moja organizácia urobiť?

Vaše IT oddelenie môže nakonfigurovať automatické aktualizácie pre operačné systémy a aplikácie používané v celej organizácii, vybrať, kedy a ako často ich nainštalovať bez prerušenia prevádzky.

Ako to spravím?

V systéme Windows
Na Macu

V systéme Android
Na IOS

Užitočné nástroje

Spravujte aktualizácie v systéme Windows

Zapnite automatické aktualizácie aplikácií

Aktualizujte MacOS na Macu

Co-funded by the European Union

3. Preventívne opatrenia

3.5. Zabezpečenie siete - VPN

Prečo je to dôležité ?

Keď je potrebné, aby pracovníci pristupovali k informáciám z **prostredia mimo priestorov** , je pre pracovníkov IT ťažšie kontrolovať **všetky bezpečnostné aspekty** . **Virtuálne privátne siete (VPN)** umožňujú vytvorenie **priamej, bezpečnej a izolovanej siete** medzi dvoma strojmi a umožňujú im interakciu a výmenu údajov.

Ako to funguje?

VPN je technológia, ktorá vytvára **bezpečné a šifrované** pripojenie cez internet. Siete VPN šifrujú údaje prenášané medzi zariadením používateľa a serverom VPN, čím bránia tretím stranám v zachytení a prístupe k údajom. Toto šifrovanie je **ďalšou vrstvou zabezpečenia** , ktorá zaisťuje, že citlivé informácie, ako sú heslá, podrobnosti o kreditných kartách a osobná komunikácia, zostanú v bezpečí.

V kontexte opatrovateľských pracovníkov budú VPN väčšinou **zabezpečovať vzdialený prístup** k súkromným sieťam a zdrojom, ako sú podnikové intranety, servery alebo databázy, najmä pre tých, ktorí pracujú v teréne. Poskytnú tiež **zvýšenú bezpečnosť** pre tých, ktorí sa pripájajú k internetu cez **verejné** a všeobecne nezabezpečené **Wifi siete** .

Co-funded by the European Union

3. Preventívne opatrenia

3.5. Zabezpečenie siete - VPN

Prečo je to dôležité ?

Keď je potrebné, aby pracovníci pristupovali k informáciám z **prostredia mimo priestorov** , je pre pracovníkov IT ťažšie kontrolovať **všetky bezpečnostné aspekty** . **Virtuálne privátne siete (VPN)** umožňujú vytvorenie **priamej, bezpečnej a izolovanej siete** medzi dvoma strojmi a umožňujú im interakciu a výmenu údajov.

Čo môže moja organizácia urobiť?

Siete VPN by malo v prípade potreby inštalovať **technické oddelenie organizácie** , pretože sa väčšinou budú používať ako **celosystémové geografické rozšírenie existujúcej siete** , čo bráni jednotlivým používateľom v ich autonómnej inštalácii. Jednotlivci však môžu **obhajovať** VPN svojmu oddeleniu IT alebo manažmentu.

Siete VPN môžu vyžadovať **inštaláciu softvéru** na počítačoch, ktoré je potrebné prepojiť, ako aj **metódu overovania** pred prístupom k sieti. Môžu byť nakonfigurované tak, aby fungovali iba na určitých zariadeniach, na určitých miestach a v určitých časoch, aby obmedzili externý prístup a zároveň poskytli pracovníkom, ktorí to potrebujú, prístup k potrebným údajom.

Co-funded by the European Union

3. Preventívne opatrenia

3.6. Zálohovanie dát

Prečo je to dôležité?

Jednou z hlavných hrozieb kybernetických útokov je **zmena citlivých údajov** , konkrétne údajov o pacientoch. Zabezpečenie jeho bezpečnosti a integrity je absolútne dôležité, a to aj zoči-voči kybernetickej hrozbe. Kľúčom k zabezpečeniu integrity údajov je robustná **inštitucionálna stratégia zálohovania údajov** s pravidelnými **zálohovacími postupmi** a **vysokými zamestnancami.**

Čo môžem urobiť?

- Ako jednotliví pracovníci je prvým opatrením na zaistenie integrity a bezpečnosti údajov **dodržiavanie rôznych protokolov** stanovených technickým oddelením, **pravidelné školenia** a seriózne a dôsledné **zvažovanie tejto záležitosti.**
- Ako aktér zabezpečenia vlastnej organizácie sa môžete tiež **informovať** o svojej stratégii zálohovania údajov, **navrhovať** a **obhajovať** úpravy.

Čo môže moja organizácia urobiť?

Navrhovanie a realizácia an **inštitucionálna stratégia zálohovania dát** je v kompetencii technického oddelenia. Takáto stratégia by mala zahŕňať **opatrenia zabezpečujúce dodržiavanie predpisov zo strany zamestnancov** , postupy **pravidelného zálohovania údajov** na **riešeniach cloudového úložiska** (GoogleDrive, OneDrive atď.) alebo sieťovom úložisku, ktoré poskytujú bezpečnostnú sieť na **rýchlu obnovu údajov** v prípade narušenie spochybňovania integrity údajov.

Co-funded by the European Union

SociALL

4. Osvedčené postupy a dobré návyky

1. Fyzický priestor
2. Bezpečné prehliadávanie
3. Bezpečné posielanie e-mailov
4. Bezpečné používanie sociálnych médií
5. Mobilné zariadenie bezpečnosť
6. Zabezpečenie heslom

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPWA
Medical Car
åpenhet
Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.1. Fyzický priestor

Kybernetická bezpečnosť začína offline : pred nastavením technickej ochrany sa uistite, že ste svoj fyzický priestor usporiadali bezpečným spôsobom, čím sa znížia nebezpečenstvá a zraniteľné miesta.

1. Zamknite svoje zariadenia, keď ich nepoužívate
2. Zabezpečte svoj pracovný priestor pred neoprávneným prístupom
3. Prijmite zásady čistého pracovného stola
4. Používajte ochranné obrazovky
5. Skartujte citlivé dokumenty
6. Nezapisujte si heslá
7. Majte na pamäti surfovanie na ramenách
8. Povoliť šifrovanie celého disku

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.1. Fyzický priestor

Kybernetická bezpečnosť začína offline: pred nastavením technickej ochrany sa uistite, že ste svoj fyzický priestor usporiadali bezpečným spôsobom, čím sa znížia nebezpečenstvá a zraniteľné miesta.

1. Zamknite svoje zariadenia, keď ich nepoužívate

Vždy **uzamknite** svoj počítač, notebook, tablet alebo telefón, keď ich nepoužívate, najmä na verejných alebo spoločných priestoroch. Na zabezpečenie svojich zariadení a zabránenie neoprávnenému prístupu používajte silné heslá, kódy PIN alebo biometrické overenie (napr. pomocou odtlačkov prstov alebo rozpoznávania tváre).

Tipy

- V systéme Windows použite skratku Windows + L na uzamknutie obrazovky .
- Na Macu použite skratku Control-Command-Q na uzamknutie obrazovky.

2. Zabezpečte svoj pracovný priestor pred neoprávneným prístupom

- Udržujte svoj pracovný priestor **bez neoprávnených osôb**. Uistite sa, že fyzické prístupové body, ako sú dvere, okná alebo vchody, sú zabezpečené a monitorované, aby sa zabránilo neoprávnenému vstupu do vášho pracovného priestoru alebo priestorov.
- **Zamknite** zásuvky, skrinky alebo kartotéky obsahujúce citlivé dokumenty, zariadenia alebo pamäťové médiá, keď sa nepoužívajú.
- Zabezpečte **periférne zariadenia** , ako sú klávesnice, myši a externé úložné zariadenia (USB, pevný disk atď.) a uložte ich do uzamknutých zásuviek alebo skriniek.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.1. Fyzický priestor

Kybernetická bezpečnosť začína offline: pred nastavením technickej ochrany sa uistite, že ste svoj fyzický priestor usporiadali bezpečným spôsobom, čím sa znížia nebezpečenstvá a zraniteľné miesta.

3. Prijmite zásady čistého pracovného stola

Dodržiavajte **zásady čistého pracovného stola** odstránením citlivých dokumentov, poznámok alebo hesiel zo svojho stola, keď nie ste prítomní. Fyzické dokumenty uchovávajte bezpečne, najlepšie v uzamknutých skrinkách alebo zásuvkách.

Tipy

Dobrou praxou je mieriť pre „0-papierový stôl“, pričom na stole sa momentálne používajú iba papiere. Nielenže je preukázané, že zvyšuje efektivitu a znižuje stres, ale tiež znižuje riziko, že dôležité informácie budú viditeľné pre neoprávnené osoby.

4. Používajte ochranné obrazovky

Používajte **obrazovky alebo filtre ochrany osobných údajov** na počítači alebo mobilných zariadeniach, aby ste zabránili neoprávnenému prezeraniu obrazovky. Ochranné obrazovky nútia divákov byť presne pred zariadením a zabraňujú surfovaniu cez rameno. Sú zabudované v určitých zariadeniach alebo sa dajú stiahnuť.

Tipy

- Na počítačoch s vstavaný privátne obrazovky aktivujte stlačením F12 alebo Fn + D to .
- V systéme Android, najlepšie hodnotené Aplikácie na ochranu súkromia sú 1) Privacy Screen, 2) Screen Guard Privacy , 3) Privacy filter.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.1. Fyzický priestor

Kybernetická bezpečnosť začína offline: pred nastavením technickej ochrany sa uistite, že ste svoj fyzický priestor usporiadali bezpečným spôsobom, čím sa znížia nebezpečenstvá a zraniteľné miesta.

5. Skartujte citlivé dokumenty

Pred vyradením **skartujte alebo bezpečne zlikvidujte fyzické dokumenty obsahujúce citlivé informácie, ako sú finančné záznamy, osobná identifikácia atď.** Nehádžte jednoducho do koša bez toho, aby ste dokument **aspoň neroztrhli.**

Tipy

Zatiaľ čo recyklácia je akýkoľvek robotníckeho zodpovednosť dnes , pamätajte že Voľný papier je často ponechaný bez dozoru pred jeho recykláciou a môže spôsobiť, že vaša organizácia bude zraniteľná voči potenciálnemu narušeniu bezpečnosti, ak je citlivá.

6. Nezapisujte si heslá

Nezapisujte si heslá ani kódy PIN na poznámkové bloky, poznámkové bloky alebo fyzické dokumenty. Ak je absolútne nevyhnutné napísať heslo, urobte tak na mieste, kde ho nemožno nájsť a zašifrujte ho kódom, ktorý dokážete rozlúštiť iba vy (napr.: počet detí sestry/mesiac narodenín psa atď.)

Tipy

Namiesto toho použite na bezpečné ukladanie a správu hesiel renomovaného správcu hesiel. Jediné heslo, ktoré si budete musieť zapamätať, je heslo správcu hesiel.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.1. Fyzický priestor

Kybernetická bezpečnosť začína offline : pred nastavením technickej ochrany sa uistite, že ste svoj fyzický priestor usporiadali bezpečným spôsobom, čím sa znížia nebezpečenstvá a zraniteľné miesta.

7. Dávajte pozor na surfovanie na ramenách

Dávajte pozor na svoje okolie a chráňte svoju obrazovku a klávesnicu pred nepovolanými osobami, najmä na verejných priestranstvách. **Chráňte si klávesnicu** pri zadávaní PIN alebo hesiel na bankomatoch, klávesniciach alebo mobilných zariadeniach.

Tipy

- Ochranné obrazovky sú dobrým spôsobom boja proti rameno surfovanie.
- Keď ste vo verejnom priestore, privilégium sedenie s chrbtom k stene.

8. Povoľte šifrovanie celého disku

Povoľte na svojich zariadeniach **šifrovanie celého disku** , aby ste ochránili údaje uložené na pevnom disku alebo pamäťovom médiu zariadenia. To zaisťuje, že aj keď je vaše zariadenie odcudzené alebo stratené, neoprávnení používatelia nebudú mať prístup k údajom bez šifrovacieho kľúča.

Tipy

- V systéme Windows povoľte šifrovanie v časti Nastavenia > Ochrana osobných údajov a zabezpečenie.
- Väčšina mobilných operačných systémov v súčasnosti disponuje aj funkciami umožňujúcimi vzdialené vymazanie údajov v prípade straty zariadenia.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.2. Bezpečné prehladávanie

Pri **prehliadaní** internetu sa uistite, že dodržiavate nasledujúce osvedčené postupy.

1. Používajte zabezpečené webové stránky (HTTPS)
2. Udržujte svoj softvér a operačný systém aktuálny
3. Používajte blokátory reklám a filtre obsahu
4. Buďte opatrní pri sťahovaní
5. Prehliadajte anonymne
6. Pravidelne vymazávajte vyrovnávaciu pamäť prehliadača a súbory cookie

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.2. Bezpečné prehliadanie

Pri **prehliadaní** internetu sa uistite, že dodržiavate nasledujúce osvedčené postupy.

1. Používajte zabezpečené webové stránky (HTTPS)

Ak chcete zabezpečiť bezpečné pripojenie pri prenose citlivých informácií, ako sú prihlasovacie údaje alebo finančné údaje, vyhľadajte v adrese URL webových stránok **HTTPS .** Vyhnite sa zadávaniu osobných údajov na webových stránkach, ktoré používajú iba **HTTP**.

Tipy

HTTP správy sú prostý text, čo znamená, že neoprávnené strany k nim môžu ľahko pristupovať a čítať ich cez internet. HTTPS prenáša všetky dáta v šifrovanej podobe. Keď používatelia odosielajú citlivé údaje, žiadne tretie strany nemôžu zachytiť údaje cez sieť.

2. Udržujte svoj softvér a operačný systém v aktuálnom stave

Pravidelne aktualizujte svoj operačný systém (OS), webový prehliadač, antivírusový softvér a ďalšie aplikácie, aby ste opravili známe zraniteľnosti a chránili pred bezpečnostnými hrozbami.

Tipy

Keď dostanete upozornenie na aktualizáciu, neodkladajte aktualizáciu všetkého softvéru a aplikácií, ktoré používate (osobne aj profesionálne). Pravidelne overujte, či je všetko aktuálne vo vašom aplikačnom centre.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.2. Bezpečné prehliadanie

Pri **prehliadaní** internetu sa uistite, že dodržiavate nasledujúce osvedčené postupy.

3. Používajte blokátory reklám a filtre obsahu

Nainštalujte si **blokátory reklám a filtre obsahu** , aby ste zabránili škodlivým reklamám, kontextovým oknám alebo skriptom ohroziť vaše prehliadanie alebo poskytovať škodlivý softvér. Niektoré webové stránky môžu vyžadovať, aby ste ich deaktivovali, aby ste získali prístup k obsahu, čo sa dá jednoducho urobiť pomocou ikony vo vašom prehliadači.

Tipy

Najlepšie hodnotené bezplatné blokátory reklám:

- uBlock pôvodu
- Ochrana osobných údajov Badger
- Ghostery
- Adblock plus

4. Buďte opatrní pri sťahovaní

Sťahujte softvér, súbory a prílohy iba z **dôveryhodných zdrojov** a vyhýbajte sa sťahovaniu obsahu z nedôveryhodných webových stránok alebo neznámych zdrojov, aby ste minimalizovali riziko infekcie škodlivým softvérom.

Tipy

Neuveriteľné množstvo obsahu je dostupné na internete. Ak webová stránka vyžaduje ak si chcete niečo stiahnuť , pravdepodobne môžete prístup podobný obsah z ďalší webové stránky , bez sťahovanie čokoľvek.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.2. Bezpečné prehliadanie

Pri **prehliadaní** internetu sa uistite, že dodržiavate nasledujúce osvedčené postupy.

5. Prehliadajte anonymne

Zvážte použitie **virtuálnej súkromnej siete (VPN)** na **šifrovanie** vášho internetového prenosu a anonymné prehliadanie, najmä pri používaní verejných sietí Wi-Fi alebo pri prístupe k citlivým informáciám.

Tipy

Nezamieňajte si režim „inkognito“ alebo režim „súkromného prehliadania“ za sieť VPN: nerobia vaše prehliadanie o nič bezpečnejším: jednoducho vymažú vašu históriu prehliadania z vášho zariadenia. Ale vaša história prehliadania je stále viditeľná pre vonkajší svet, rovnako ako vaša IP adresa, sieť atď.

6. Pravidelne čistite vyrovnávaciu pamäť prehliadača a súbory cookie

Pravidelne **čistite** vyrovnávaciu pamäť prehliadača, súbory cookie a históriu prehliadania, aby ste odstránili **údaje zo sledovania** a minimalizovali riziko neoprávneného prístupu k vašim zvykom prehliadania alebo osobným informáciám.

Tipy

V prehliadači Chrome kliknite na 3 bodky v pravom hornom rohu > Odstrániť údaje prehliadania. Na novo otvorenej karte vyberte obdobie, za ktoré chcete vymazať údaje (ideálne „Celé obdobie“), vyberte tri možnosti (história prehliadania, súbory cookie a vyrovnávacia pamäť) a kliknutím na „Odstrániť údaje prehliadania“ okamžite vymažte prehliadač.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.3. Bezpečné posielanie e-mailov

Keď dostanete e-mail, nezabudnite si položiť nasledujúce otázky, aby ste predišli akýmkoľvek bezpečnostným problémom:

1. Poznám a rozpoznám odosielateľa?
2. Je e-mail neočakávaný alebo nevyžiadaný?
3. Oslovuje ma e-mail menom?
4. Sú tam pravopisné alebo gramatické chyby?
5. Existujú podozrivé prílohy?
6. Obsahuje e-mail neočakávané odkazy?
7. Žiada e-mail o citlivé informácie?
8. Vyzerajú podpis a kontaktné údaje legitímne?
9. Mám existujúci vzťah s odosielateľom?
10. Používa e-mail hrozby alebo taktiku strachu?
11. Zistil antivírus niečo podozrivé?
12. Vyzerá to ako iné e-maily od tohto poskytovateľa?

Okrem toho sa vždy uistite, že k e-mailu pristupujete **takto**:

- nepodnikajte **okamžité, unáhlené opatrenia**
- **Vždy predpokladajte** , že e-mail môže byť **podvod** , vezmite si čas na jeho preštudovanie a „vyčistite“.
- **Dôverujte svojmu úsudku** a inštinktom: ak sa vám niečo nezdá, skúmajte to opatrne.
- Pamätajte, že podvody hrajú na **emócie** , ako je strach, prostredníctvom zastrašovania a vyhrážok. Zachovajte **chladnú hlavu** a zachovajte **pokoj** vo všetkých prípadoch.

Co-funded by the European Union

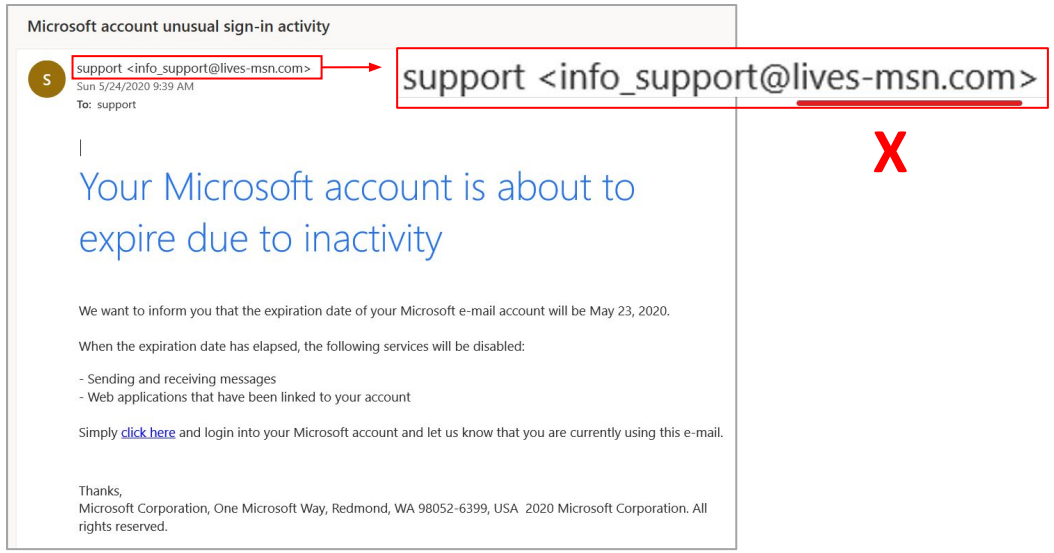
4. Osvedčené postupy a dobré návyky

4.3. Bezpečné posielanie e-mailov

Keď dostanete e-mail, nezabudnite si položiť nasledujúce otázky, aby ste predišli akýmkoľvek bezpečnostným problémom:

1. Poznám a rozpoznám odosielateľa?

Overte totožnosť odosielateľa, a to nielen zobrazením mena zobrazeného navrchu a v podpise, ale aj **skutočnej e-mailovej adresy**, ktorá e-mail odoslala.



X

2. Je e-mail neočakávaný alebo nevyžiadaný?

Dávajte si pozor na neočakávané e-maily, najmä tie, ktoré požadujú **naliehavé opatrenia** alebo ponúkajú **nevyžiadané služby**. Podvodníci ich často používajú na oklamanie príjemcov, pričom najčastejšie používajú tieto témy:

- Potrebujete aktualizovať alebo overiť informácie o účte (pozastavenie účtu, vypršanie platnosti, bezpečnostné upozornenie atď.)
- Potrebujete zaplatiť čakajúcu faktúru prostredníctvom odkazu
- Ponuky falošných pracovných príležitostí
- Platba alebo vzdialený prístup k počítaču alebo účtu požadované „podporou“ na vyriešenie technických problémov.
- Ak chcete získať nevyžiadanú odmenu alebo cenu, musíte zaplatiť poplatky za spracovanie alebo poskytnúť osobné údaje.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

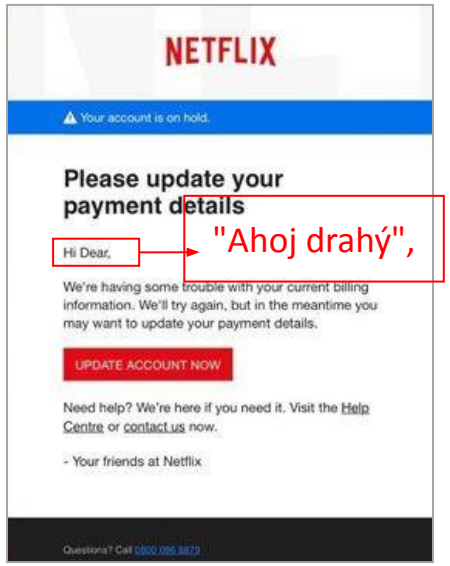
SociALL

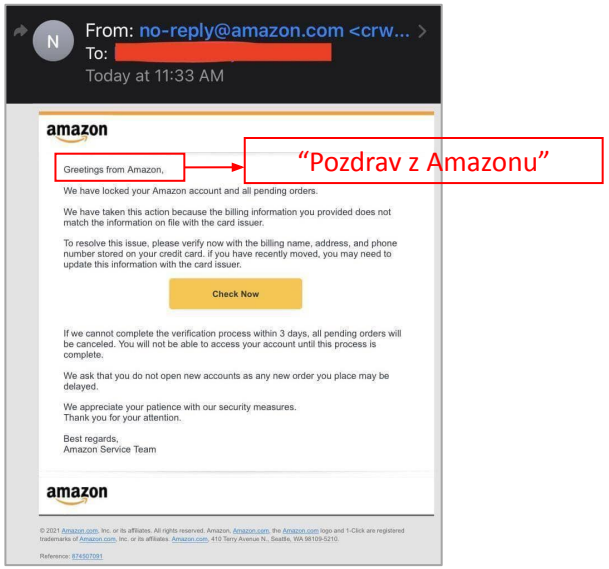
4.3. Bezpečné posielanie e-mailov

Keď dostanete e-mail, nezabudnite si položiť nasledujúce otázky, aby ste predišli akýmkoľvek bezpečnostným problémom:

3. Oslovuje ma e-mail menom?

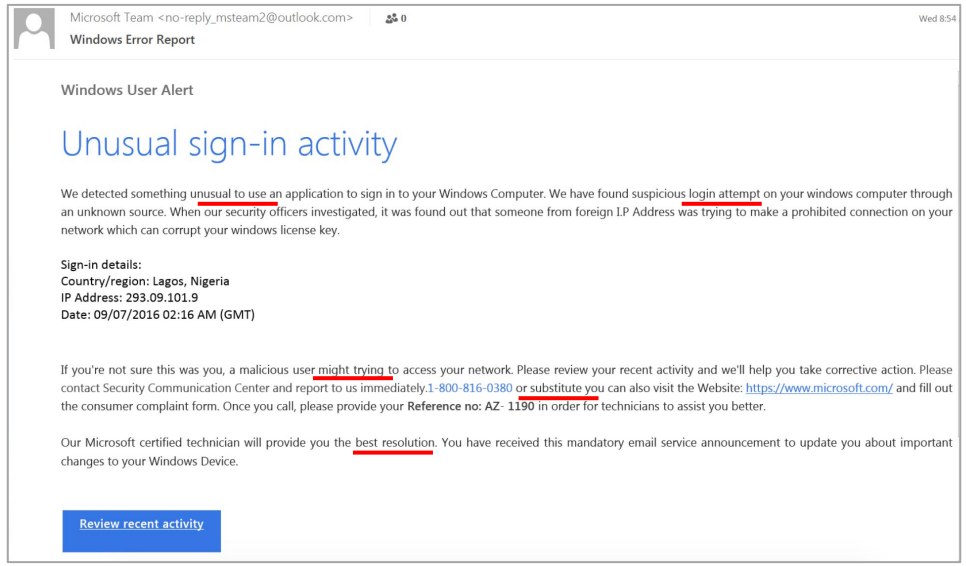
Legitímne organizácie často používajú vaše meno vo svojej komunikácii. **Všeobecné pozdravy** alebo **nesprávne napísané** vaše meno môžu byť červené vlajky.





4. Vyskytujú sa pravopisné alebo gramatické chyby?

Zle napísané e-maily s **pravopisom** alebo **gramatikou chyby** môžu naznačovať pokus o phishing. Legitímne organizácie vo všeobecnosti robia menej chýb vo svojich e-mailoch.



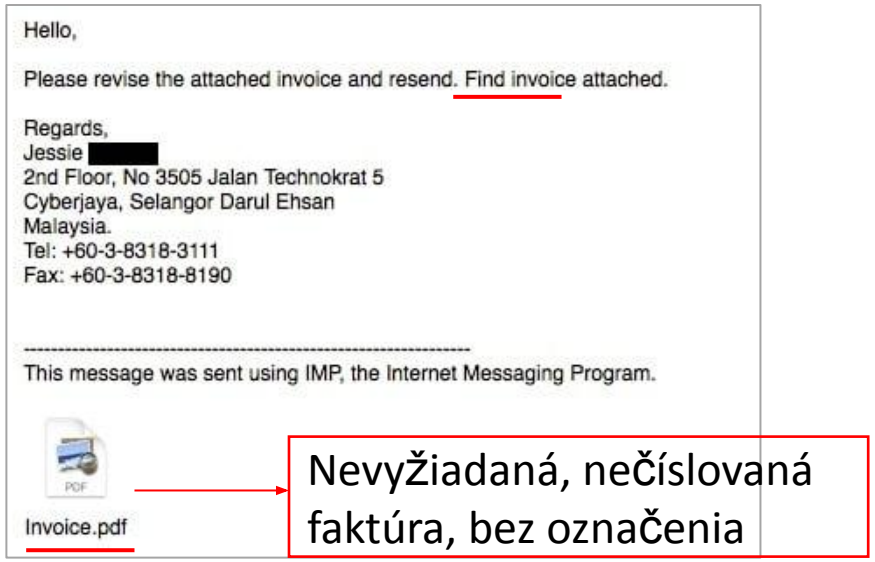
4. Osvedčené postupy a dobré návyky

4.3. Bezpečné posielanie e-mailov

Keď dostanete e-mail, nezabudnite si položiť nasledujúce otázky, aby ste predišli akýmkoľvek bezpečnostným problémom:

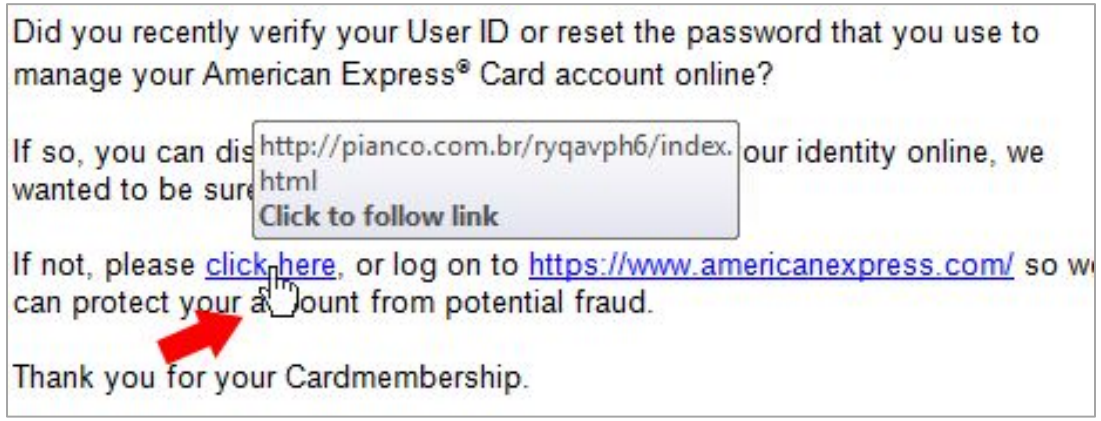
5. Existujú podozrivé prílohy?

Vyhnite sa otváraniu **neočakávaných príloh** , najmä z neznámych zdrojov. Škodlivé prílohy môžu obsahovať **malvér** alebo pokusy **o phishing**.



6. Obsahuje e-mail neočakávané odkazy?

Ak chcete zobraziť **skutočnú adresu URL, umiestnite kurzor myši na akýkoľvek odkaz v e-maile bez kliknutia** . Ak sa odkaz nezhoduje s oficiálnou webovou stránkou údajného odosielateľa alebo vyzerá podozrivo, môže ísť o pokus o phishing.



JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Co-funded by the European Union

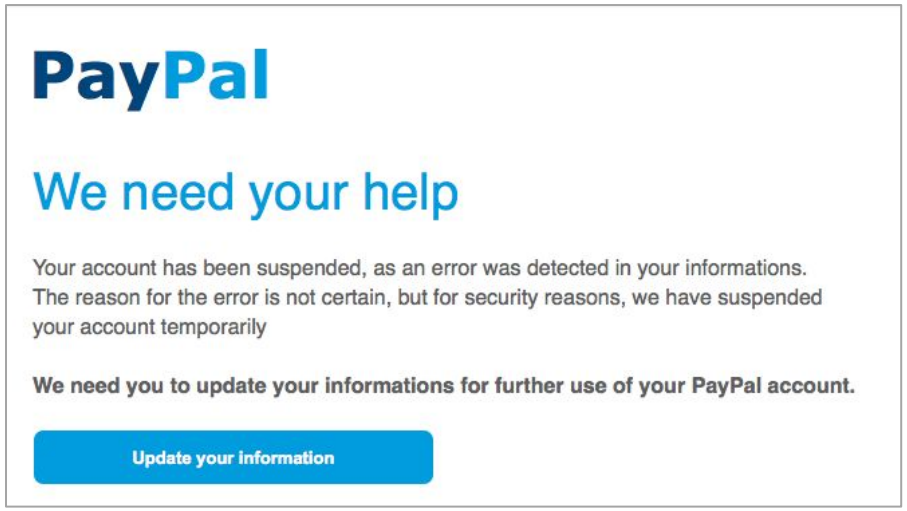
4. Osvedčené postupy a správne návyky

4.3. Bezpečné posielanie e-mailov

Keď dostanete e-mail, nezabudnite si položiť nasledujúce otázky, aby ste predišli akýmkoľvek bezpečnostným problémom:

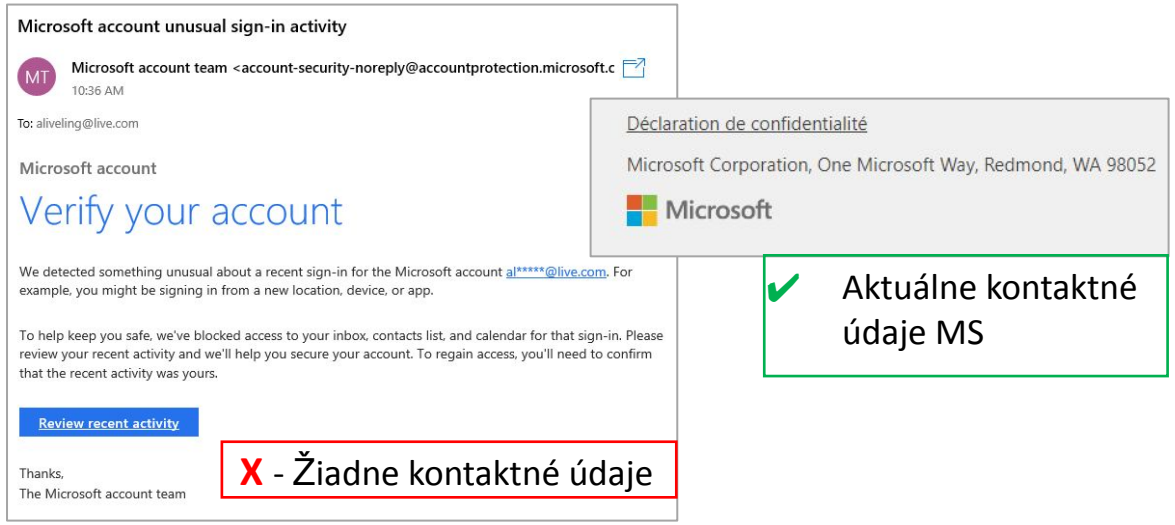
7. Žiada e-mail o citlivé informácie?

Organizácie zvyčajne **nepožadujú citlivé informácie** e **-mailom** alebo prostredníctvom **odkazu** (ako sú heslá alebo podrobnosti o kreditných kartách), ale zvyčajne vás vyzývajú, aby ste sa pripojili k **svojmu účtu** na svojich webových stránkach.



8. Vyzerajú podpis a kontaktné údaje legitímne?

Legitímne organizácie zvyčajne poskytujú vo svojich e-mailoch **jasné kontaktné informácie** vrátane **fyzickej adresy** . Overte podrobnosti odosielateľa vrátane jeho **podpisu** a porovnajte ich s oficiálnymi zdrojmi.



JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medical car
åpenhet
Co-funded by the European Union

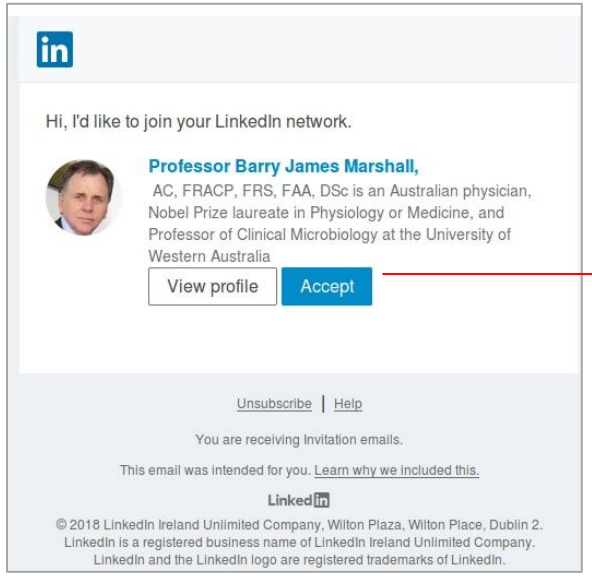
4. Osvedčené postupy a správne návyky

4.3. Bezpečné posielanie e-mailov

Keď dostanete e-mail, nezabudnite si položiť nasledujúce otázky, aby ste predišli akýmkoľvek bezpečnostným problémom:

9. Mám existujúci vzťah s odosielateľom?

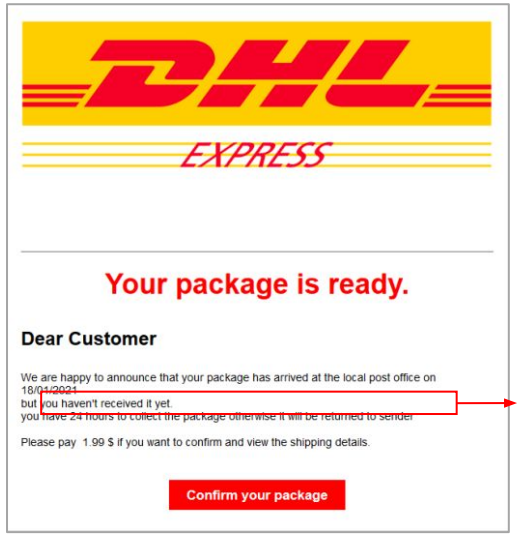
Ak e-mail tvrdí, že pochádza od organizácie, v ktorej máte účet, overte si informácie **zo svojho účtu** a nespoliehajte sa iba na e-mail.



Namiesto kliknutia na „Prijať“ skontrolujte účet LinkedIn

10. Používa e-mail hrozby alebo taktiku strachu?

Podvodníci používajú taktiky **vyhrážok** , **zastrašovania** alebo **strachu** , aby dotlačili príjemcov k rýchlej akcii. Dávajte si pozor na e-maily, ktoré vyvolávajú pocit **naliehavosti** alebo **strachu**.



„Na vyzdvihnutie balíka máte 24 hodín, inak bude vrátený odosielateľovi“

Co-funded by the European Union

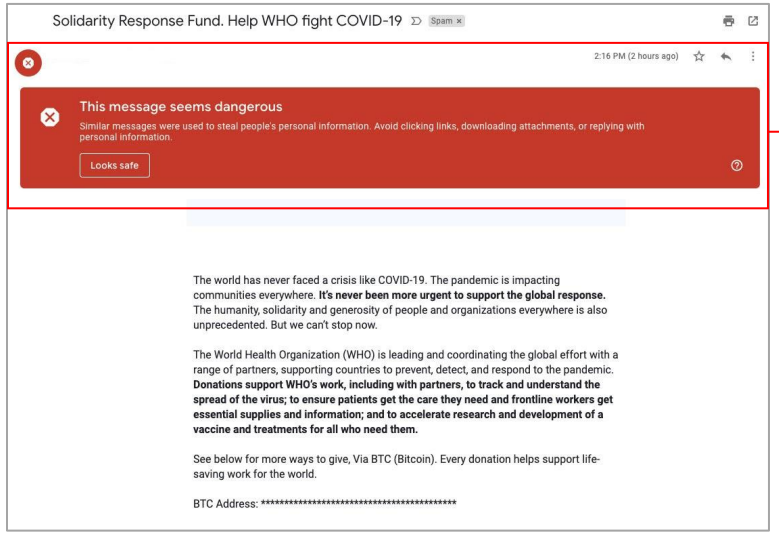
4. Osvedčené postupy a dobré návyky

4.3. Bezpečné posielanie e-mailov

Keď dostanete e-mail, nezabudnite si položiť nasledujúce otázky, aby ste predišli akýmkoľvek bezpečnostným problémom:

11. Zistil antivírus niečo podozrivé?

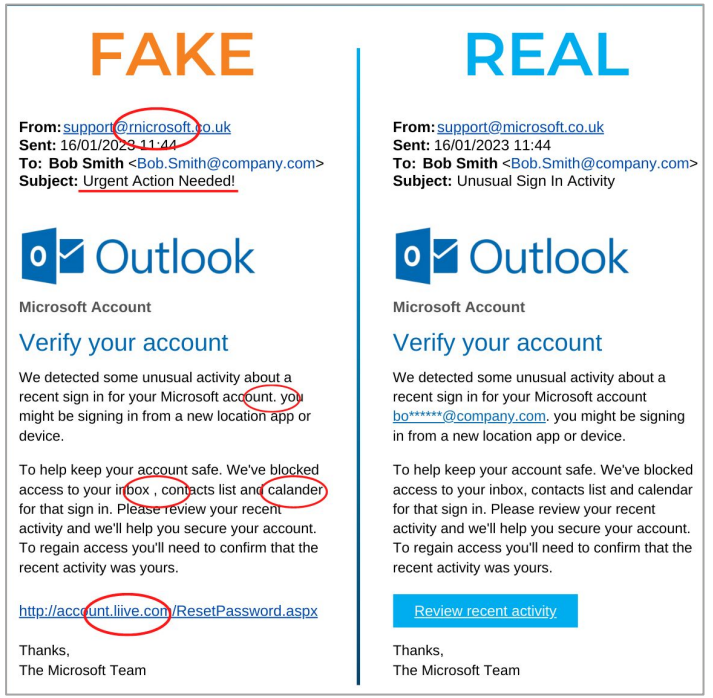
Väčšina poskytovateľov e-mailu má **vstavané moduly** zisťujúce pokusy o phishing. Okrem toho váš vlastný **antivírus** mohol označiť e-mail ako **podozrivý** . Ak áno, postupujte s e-mailom **opatrne.**



„Táto správa sa zdá byť nebezpečná“

12. Vyzerá to ako iné e-maily od tohto poskytovateľa?

Pri prijímaní e-mailu pravdepodobne od organizácie, od ktorej ste **už e-maily dostali** , pred dôverou si overte, či sa dizajn, značka, kontaktné údaje, autorské práva, odkazy a jazyk **zhodujú**.



Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.4. Bezpečné používanie sociálnych médií

Bezpečne používajte sociálne médiá integrovaním nasledujúcich postupov.

1. Skontrolujte a upravte nastavenia ochrany osobných údajov
2. Buďte selektívni pri žiadostiach o priateľstvo a spojeniach
3. Dajte si pozor na phishing a podvody
4. Dávajte pozor na zdieľanie polohy a na to, čo uverejňujete
5. Overte pravosť účtu
6. Monitorujte aplikácie a povolenia tretích strán

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.4. Sociálne médiá a správy

Bezpečne používajte sociálne médiá integrovaním nasledujúcich postupov.

1. Skontrolujte a upravte nastavenia ochrany osobných údajov

Pravidelne **kontrolujte a upravujte svoje nastavenia ochrany osobných údajov** na platformách sociálnych médií, aby ste mali kontrolu nad tým, kto môže vidieť vaše príspevky, osobné informácie a fotografie.
Obmedzte publikum pre svoje príspevky a zvážte **obmedzenie prístupu** k citlivým informáciám na dôveryhodných priateľov a kontakty.

Tipy

Väčšina predvolených nastavení ochrany osobných údajov na sociálnych médiách môže povoliť zdieľanie vašich informácií s inými online používateľmi tretích strán vrátane vášho mena, veku, miesta bydliska, pohlavia atď.

2. Buďte selektívni pri žiadostiach o priateľstvo a spojeniach

Buďte opatrní pri prijímaní **žiadostí o priateľstvo alebo spojení** od neznámych osôb. Pred prijatím žiadosti overte totožnosť osoby, najmä ak ju osobne nepoznáte. Mnoho podvodov na sociálnych sieťach začína tým, že sa stanete „vaším priateľom“ a **získate prístup k viacerým vašim údajom** .

Tipy

Pokúste sa overiť pravosť. Príklad: Ak dostanete žiadosť od niekoho, kto tvrdí, že je bratom vášho priateľa, môžete požiadať svojho priateľa, aby pred prijatím potvrdil totožnosť osoby.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.4. Sociálne médiá a správy

Bezpečne používajte sociálne médiá integrovaním nasledujúcich postupov.

3. Dajte si pozor na phishing a podvody

Dávajte **si pozor na nevyžiadané** správy, odkazy alebo žiadosti od neznámych osôb na sociálnych sieťach. **Vyhnite sa klikaniu na podozrivé odkazy** alebo sťahovaniu príloh z neznámych zdrojov, pretože môžu viesť k phishingovým podvodom alebo infekciám škodlivým softvérom.

Tipy

Veľa podvodov na sociálnych sieťach stať prostredníctvom hacknutia účtu jedného z vašich kontaktov. Byť opatrný keď odošle kontakt, ktorý poznáte vy nevyžiadané, nezvyčajné žiadosti (ako je finančná podpora pre ich príbuzných v nemocnici) a overiť s ich cez iné médium).

4. Dávajte pozor na zdieľanie polohy a na to, čo uverejňujete

Obmedzte zdieľanie polohy na platformách sociálnych médií, najmä pri uverejňovaní fotografií alebo aktualizácií v reálnom čase. Vyhnite sa prezradeniu vašej presnej polohy alebo zdieľaniu osobných údajov, ktoré by mohli ohroziť vašu bezpečnosť.

Tipy

Veľa druhov informácií používajú počítačoví zločinci na spôsobenie škody . Nabok od zrejmých (meno, vek, pohlavie, mesto bydliska atď.), mnohé detaily môžu byť používané počítačovými zločincami, ako napríklad meno najbližšieho _ školy, bývalé alebo súčasné pracovisko, snímky obrazovky s osobnými údajmi a pod.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.4. Sociálne médiá a správy

Bezpečne používajte sociálne médiá integrovaním nasledujúcich postupov.

5. Overte pravosť účtu

Dávajte si pozor na **falošné účty** na platformách sociálnych médií, najmä na tie, ktoré sa vydávajú za celebrity, verejné osobnosti alebo značky. Pred interakciou s účtami alebo zdieľaním osobných údajov **overte pravosť účtov.**

Tipy

Len v roku 2021 Facebook odstránil 1,7 miliardy falošných účtov. Podobne je takmer 1 z 5 (19,42 %) odkazov na Twitteri falošný alebo spam. Modré začiarknutie „certifikujúce“ účet môže získať prakticky ktokoľvek a nie je indikátorom toho, že účtu možno dôverovať.

6. Monitorujte aplikácie a povolenia tretích strán

Pravidelne **kontrolujte a spravujte** povolenia udelené aplikáciam tretích strán pripojeným k vašim účtom sociálnych médií. Odstráňte prístup pre aplikácie, ktoré už nepoužívate alebo ktorým nedôverujete, aby ste minimalizovali riziko zneužitia údajov alebo narušenia súkromia.

Tipy

Venujte pozornosť povoleniam udeleným týmto aplikáciám, pretože môžu poskytnúť prístup k súkromným informáciám, s ktorými by nemali byť dôverné.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.5. Zabezpečenie mobilného zariadenia

Používajte svoje **mobilné zariadenie** bezpečnejšie integrovaním nasledujúcich postupov.

1. Použite zabezpečenú zámku obrazovky
2. Udržujte svoj softvér a OS aktualizované
3. Šifrovať dáta
4. Použite dôveryhodný obchod s aplikáciami
5. Skontrolujte povolenia aplikácie
6. Dávajte si pozor na verejné Wi-Fi
7. Povoliť „Nájsť moje zariadenie“
8. Obmedzte používanie Bluetooth a NFC

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.5. Zabezpečenie mobilného zariadenia

Používajte svoje **mobilné zariadenie** bezpečnejšie integrovaním nasledujúcich postupov.

1. Použite zabezpečený zámok obrazovky

Povoľte **bezpečný zámok obrazovky** (napr. PIN, heslo, vzor, biometrickú identifikáciu), aby ste zabránili neoprávnenému prístupu k vášmu zariadeniu v prípade jeho straty alebo krádeže. Nepoužívajte ľahko uhádnuteľné vzory alebo kódy PIN.

2. Udržujte svoj softvér a operačný systém aktualizované

Pravidelne **aktualizujte svoj mobilný operačný systém**, aplikácie a bezpečnostné záplaty, aby ste sa chránili pred známymi zraniteľnosťami a bezpečnostnými hrozbami. Povoľte automatické aktualizácie, aby ste zabezpečili včasné opravy zabezpečenia.

3. Šifrujte dáta

Povoľte šifrovanie údajov uložených vo vašom mobilnom zariadení na ochranu citlivých informácií. Väčšina moderných mobilných zariadení ponúka vstavané funkcie šifrovania, ktoré šifrujú dáta v pokoji.

4. Použite dôveryhodný obchod s aplikáciami

Aplikácie sťahujte iba z **oficiálnych a dôveryhodných obchodov s aplikáciami** , ako sú Apple App Store alebo Google Play Store, aby ste minimalizovali riziko sťahovania škodlivých aplikácií alebo malvéru.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.5. Zabezpečenie mobilného zariadenia

Používajte svoje **mobilné zariadenie** bezpečnejšie integrovaním nasledujúcich postupov.

5. Skontrolujte povolenia aplikácie

Skontrolujte a spravujte povolenia aplikácií, aby ste mohli ovládať, ku ktorým údajom a funkciám môžu aplikácie vo vašom zariadení pristupovať. **Zakážte nepotrebné povolenia** , ktoré aplikácie nevyžadujú pre svoju funkčnosť.

6. Dávajte si pozor na verejné Wi-Fi

Nepripájajte sa k **nezabezpečeným verejným sieťam Wi-Fi** , pretože môžu byť náchylné na odpočúvanie alebo útoky typu man-in-the-middle. Pri pripájaní k verejným sieťam Wi-Fi **použite sieť VPN na šifrovanie internetového prenosu.**

7. Povoľte „Nájsť moje zariadenie“

Povoľte na svojom mobilnom zariadení funkciu „ **Nájsť moje zariadenie** “ alebo „ **Nájsť môj iPhone** “ na vzdialenú lokalizáciu, uzamknutie alebo vymazanie zariadenia v prípade jeho straty alebo krádeže. Táto funkcia pomáha chrániť vaše údaje a súkromie v prípade krádeže alebo straty.

8. Obmedzte používanie Bluetooth a NFC

Deaktivujte Bluetooth a NFC , keď sa nepoužívajú, aby ste zabránili neoprávnenému prístupu alebo spárovaniu s inými zariadeniami. Pri párovaní s neznámymi zariadeniami buďte opatrní a používajte zariadenia Bluetooth z dôveryhodných zdrojov.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.6. Zabezpečenie heslom

Zabezpečte svoje heslá tým, že sa ubezpečíte, že obsahujú nasledujúce prvky.

1. Používajte silné a jedinečné heslá
2. Pre každý účet používajte iné heslá
3. Namiesto slov používajte prístupové frázy
4. Použite renomovaného správcu hesiel
5. Heslá vždy uchovávajte v tajnosti
6. Pravidelne aktualizujte heslá

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.6. Zabezpečenie heslom

Zabezpečte svoje heslá tým, že sa ubezpečíte, že obsahujú nasledujúce prvky.

1. Používajte silné a jedinečné heslá

Vytvárajte silné a zložité heslá, ktoré je ťažké uhádnuť. Použite kombináciu veľkých a malých písmen, číslic a špeciálnych znakov. Nepoužívajte ľahko uhádnuteľné informácie, ako sú mená, narodeniny alebo bežné slová.

Tipy

Niektoré stránky vám poskytujú informácie o bezpečnosti vášho hesla. Neregistrujte heslo, kým ho webová lokalita alebo softvér nevyhodnotí ako „silné“. Heslá by mali mať aspoň 16 znakov a miešať rôzne typy znakov.

2. Pre každý účet používajte iné heslá

Nepoužívajte rovnaké heslo pre viacero účtov. Používajte jedinečné heslá pre každý online účet, aby ste minimalizovali dopad narušenia bezpečnosti na iné účty.

Tipy

Použite správcu hesiel, aby ste si nemuseli pamätať alebo zapisovať heslá. Budete si musieť zapamätať iba heslo vášho správcu hesiel.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.6. Zabezpečenie heslom

Zabezpečte svoje heslá tým, že sa ubezpečíte, že obsahujú nasledujúce prvky.

3. Namiesto slov používajte prístupové frázy

Zvážte použitie **prístupových fráz** namiesto tradičných hesiel. Prístupové frázy sú dlhšie **kombinácie slov alebo fráz** , ktoré sa ľahšie zapamätajú, ale ťažšie sa dajú prelomiť. Napríklad „ Icàre@b0utSecur1ty! “ je silná prístupová fráza.

Tipy

Najprv vyberte prístupovú frázu, ktorú si ľahko zapamätáte. Potom si vytvorte svoj vlastný „šifrovací systém“, napríklad: o=0, i =1, a=@ atď. Nezabudnite tiež integrovať veľké písmená a špeciálne znaky.

4. Použite renomovaného správcu hesiel

Na bezpečné ukladanie a správu hesiel použite **renomovaného správcu hesiel.** Správcovia hesiel generujú silné, jedinečné heslá pre každý účet a ukladajú ich v zašifrovanom trezore, ktorý je prístupný iba s hlavným heslom.

Tipy

Príklady renomovaného správcu hesiel sú uvedené v poslednej časti tohto učebného plánu. Uistite sa, že používate funkciu generovania hesiel, aby ste mohli využívať jedinečné, silné a náhodne generované heslá, ktoré si nemusíte pamätať.

Co-funded by the European Union

4. Osvedčené postupy a dobré návyky

4.6. Zabezpečenie heslom

Zabezpečte svoje heslá tým, že sa ubezpečíte, že obsahujú nasledujúce prvky.

5. Vždy uchovávajte heslá v tajnosti

Nikdy nezdieľajte svoje heslá s nikým vrátane priateľov, rodinných príslušníkov alebo kolegov. Udržujte svoje heslá v tajnosti a vyhýbajte sa ich zapisovaniu alebo ukladaniu na ľahko prístupných miestach. Nezabudnite ich uložiť v správcovi hesiel.

Tipy

Ak je nevyhnutné zdieľať heslo, najlepšie je to urobiť ústne alebo alternatívne prostredníctvom zabezpečenej, šifrovanej aplikácie (napr.: nikdy nie cez kanál sociálnych médií). Nikdy nezdieľajte prihlasovacie meno / e-mailovú adresu prostredníctvom rovnakej aplikácie a robte tak prostredníctvom iného média.

6. Pravidelne aktualizujte heslá

Pravidelne aktualizujte svoje heslá pre online účty, najmä pre citlivé účty, ako sú bankovníctvo, e-maily alebo účty sociálnych médií. Okamžite zmeňte heslá, ak máte podozrenie, že mohli byť prezradené, a nechajte správcu hesiel pravidelne vytvárať nové.

Tipy

Nezabudnite zmeniť predvolené heslá, ktoré sa dodávajú so zariadeniami, smerovačmi alebo softvérovými aplikáciami. Predvolené heslá sa často dajú ľahko uhádnuť a sú všeobecne známe, vďaka čomu sú zraniteľné voči neoprávnenému prístupu.

Co-funded by the European Union

SociALL

5. Užitočné nástroje a dodatočné zdroje

1. Správcovia hesiel
2. 2FA nástroje
3. Anti malware
4. Šifrovanie nástrojov
5. Iné nástroje

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscar
åpenhet
Co-funded by the European Union

5. Užitočné nástroje a dodatočné zdroje

5.1. Správcovia hesiel

LastPass 1Password NordPass® KEEPER®

Správcovia hesiel **bezpečne ukladajú a spravujú heslá** naprieč rôznymi účtami, čím zjednodušujú prístup a zároveň zabezpečujú vytváranie silných, jedinečných hesiel a bezpečný prístup. Uistite sa, že:

- **Vyberte si silné, jedinečné a zapamätateľné hlavné heslo** , ktoré vám umožní prístup k správcovi hesiel. Nezabudnite si to zapamätať a nikdy to nekomunikujte; sú to dvere ku všetkým vašim účtom.
- **Nechajte správcu hesiel generovať silné, jedinečné heslá** pre každý z vašich účtov. Zapamätá si ich a uloží a už nikdy nebudete mať rovnaké heslo dvakrát.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. MPWA Medical Car åpenhet Co-funded by the European Union

5. Užitočné nástroje a dodatočné zdroje

5.2. Nástroje

Nástroje dvojfaktorovej autentifikácie (2FA) zvyšujú bezpečnosť účtu tým, že nútia používateľa, aby overil svoje prihlásenie na dvoch rôznych, registrovaných a dôveryhodných zariadeniach, zvyčajne na telefóne a počítači.

5. Užitočné nástroje a dodatočné zdroje

5.3. Anti-malwares

Anti-malware alebo antivírusy identifikujú a odstraňujú rôzne typy malvéru a poskytujú ochranu zariadení a sietí pred kybernetickými hrozbami v reálnom čase.

5. Užitočné nástroje a dodatočné zdroje

5.4. Šifrovanie nástrojov

Šifrovacie nástroje vytvárajú šifrované kontajnery, ktoré chránia citlivé súbory a priečinky tým, že bránia neoprávnenému prístupu prostredníctvom šifrovania. Niektoré nástroje, ako napríklad Bitlocker, šifrujú externé periférne zariadenia, ako je pevný disk, aby sa zvýšila ich bezpečnosť.

5. Užitočné nástroje a dodatočné zdroje

5.5. Iné užitočné nástroje

názov	Typ	Popis
Ochrana osobných údajov Badger	Rozšírenie prehliadača	Privacy Badger blokuje sledovacie súbory cookie a reklamy a chráni súkromie používateľov tým, že bráni sledovačom tretích strán zhromažďovať údaje o prehliadaní.
Imprivata	Správa prístupu	Imprivata ponúka riešenia jednotného prihlásenia, ktoré profesionálom v oblasti starostlivosti umožňujú bezpečný prístup k viacerým aplikáciám pomocou jediného prihlásenia, čo zjednodušuje pracovný tok bez ohrozenia bezpečnosti.
HIPAA One	Compliance Tool	HIPAA One automatizuje súlad so zákonom HIPAA, pomáha zdravotníckym organizáciám plniť regulačné požiadavky, vykonávať hodnotenia rizík a zaisťovať bezpečnosť údajov.
Symantec Endpoint Protection	Zabezpečenie koncového bodu	Symantec Endpoint Protection ponúka komplexné zabezpečenie vrátane pokročilej ochrany pred hrozbami, antivírusových funkcií a funkcií brány firewall, ktoré chránia pred kybernetickými hrozbami v prostrediach zdravotnej starostlivosti.
TeamViewer	Prístup na vzdialenú plochu	TeamViewer umožňuje vzdialený prístup a ovládanie zariadení, pomáha vzdialenej technickej podpore, odstraňovaniu problémov a spolupráci na rôznych miestach.
Cisco AnyConnect	Nástroj VPN	Cisco AnyConnect poskytuje zabezpečené pripojenia VPN, čo umožňuje šifrovaný prístup k organizačným sieťam zo vzdialených miest a zabezpečuje prenos dát.
Adobe Sign	Platforma elektronického podpisu	Adobe Sign uľahčuje bezpečné digitálne podpisovanie dokumentov, zjednodušuje a urýchľuje proces podpisovania a zaisťuje súlad a bezpečnosť pri správe dokumentov.

Co-funded by the European Union

Ďakujeme za Vašu časť a nápady!

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.

MedicalScar

åpenhet

Co-funded by the European Union