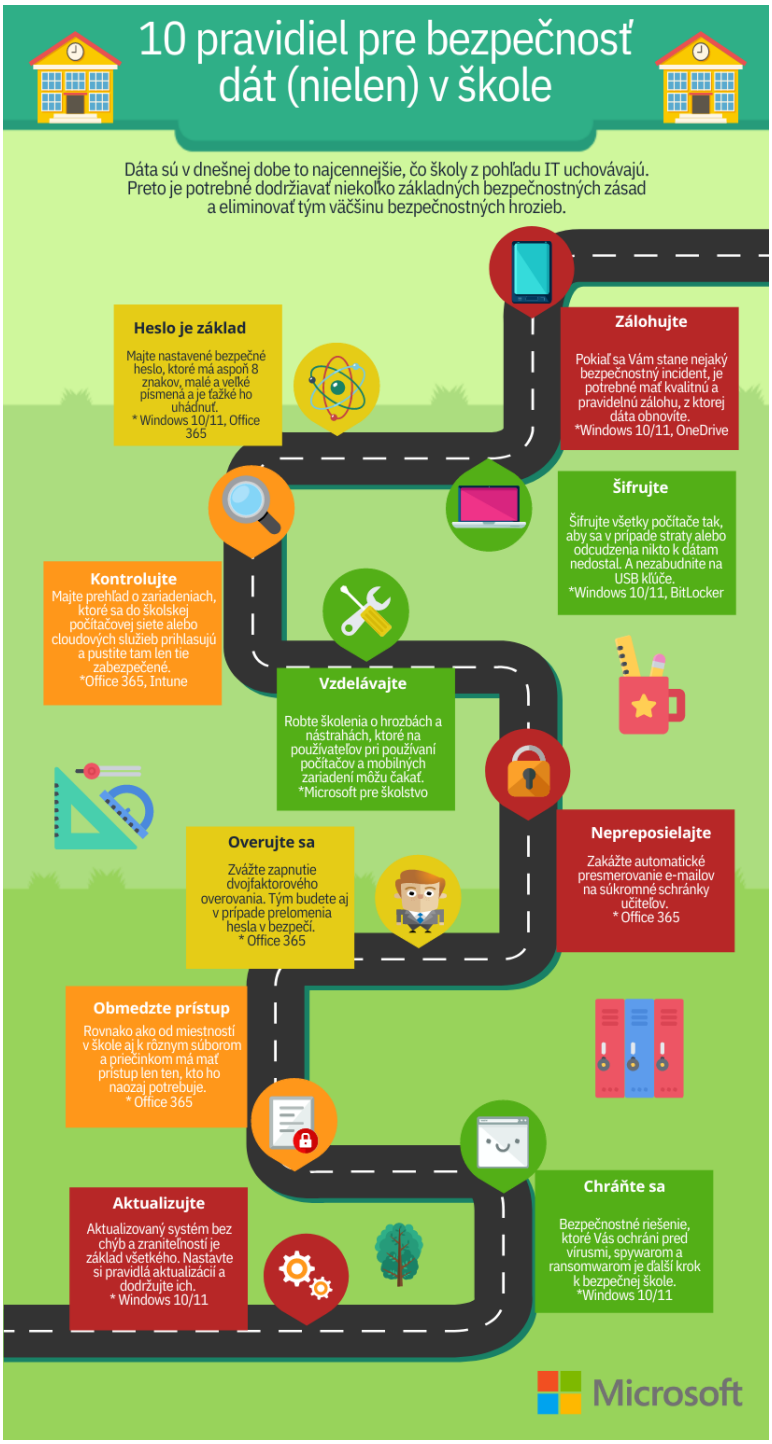
Kybernetická bezpečnosť

V tomto dokumente sa venujeme základným princípom kybernetickej bezpečnosti, ktoré sú nevyhnutné pre bezpečné fungovanie v online priestore. Najprv si vysvetlíme, čo sú cookies, ako fungujú a aký vplyv majú na naše súkromie. Potom sa pozrieme na phishing, jednu z najčastejších foriem online podvodov, a poukážeme na spôsoby, ako sa mu brániť. Ďalej sa zaoberáme dôležitosťou bezpečných hesiel a uvedieme tipy na ich tvorbu. Nakoniec sa pozrieme na metadáta, čo nám môžu prezradiť o súboroch a prečo by sme mali vedieť, ako ich spravovať.



S modernizáciou vzdelávacieho prostredia a zvyšovaním digitálnych zručností žiakov a učiteľov prichádzajú aj nové výzvy v oblasti ochrany citlivých údajov, digitálnej identity a bezpečného používania online nástrojov. Kybernetická bezpečnosť je preto kľúčovou súčasťou prebiehajúcej digitalizácie škôl na Slovensku.

Učitelia by mali byť oboznámení s rizikami, ktoré môžu ohroziť bezpečnosť digitálnych systémov ale i s osvedčenými postupmi v oblasti kybernetickej bezpečnosti, ako sú silné heslá, pravidelné aktualizácie softvéru, a vzdelávanie žiakov o bezpečnom správaní na internete. Implementácia týchto opatrení je kľúčová pre zabezpečenie hladkého priebehu digitalizácie a ochrany všetkých zúčastnených strán.

Prinášame vám základy kybernetickej bezpečnosti v príbehovej forme, aby bola táto problematika pre vás ľahšie uchopiteľná a vedeli ste tieto informácie zdieľať aj so svojimi žiakmi.

V dokumentoch ku kurzu nájdete prehľadnú inforgrafiku.

Cookies: Čo po nás zostáva online

V tejto časti sa zameriame na fungovanie cookies a na to, aké údaje o našej online aktivite zhromažďujú. V rámci podkapitoly predstavíme rôzne typy cookies, ich využitie a vplyv na naše súkromie, ako aj spôsoby, ako môžeme spravovať svoje nastavenia a chrániť sa pred neprimeraným sledovaním. Na záver sa pozrieme na regulácie, ako je GDPR, ktoré ovplyvňujú spôsob, akým sú cookies spravované a používané.

Keď navštevujeme webové stránky, často si neuvedomujeme, aké množstvo informácií o nás môže zostať uložených len tým, že sme na internete. Každý náš klik, návšteva stránky, dokonca aj čas, ktorý strávime nad jednotlivými obsahmi, vytvára stopu, ktorú môžu poskytovatelia online služieb sledovať a analyzovať. Táto stopa je známa ako cookies – súbory, ktoré zhromažďujú údaje o našom správaní na internete. Čo všetko teda o nás vedia webové stránky z týchto súborov? Je to len náš pohyb po stránkach, alebo sa za tým skrýva oveľa viac? V tejto kapitole sa ponoríme do sveta cookies a preskúmame, aké údaje zbierajú a aký dopad to môže mať na naše súkromie.

Čo všetko o mne poskytovatelia online služieb vedia len z mojej existencie na internete?

Janko a Marienka v rozprávke o perníkovej chalúpke kráčajúc lesom trúsili omrvinky a vytvorili tak cestičku, ktorá mala slúžiť ako stopa pre nich, aby sa cestou domov nestratili, alebo pre niekoho, kto by sa ich vydal hľadať. Podobne funguje internet. Chtiac, či nechtiac, pri každej online aktivite po sebe všetci zanechávame virtuálne omrvinky - **cookies**. Sú to malé info súbory, na základe ktorých poskytovatelia internetových služieb vedia vyhodnotiť, "kde v lese sme sa stratili." Tvoríme tak vlastnú **digitálnu stopu**.

Čo to znamená? Čo všetko stránky sledujú?

Poďme si spraviť malý experiment. Otvorte stránku **clickclickclick.click**. Stránka je síce v anglickom jazyku, ale zaujímavo demonštruje príklad fungovania cookies. Na stránke kliknite na zelené tlačidlo

a sledujte, ako stránka zbiera údaje o vašej aktivite. Záznam svojich činností (aj nečinností) uvidíte spísaný priamo na obrazovke. Všimnite si, ako stránka zaznamenáva:

- Pohyby myšou (kde sa nachádza, či sa kurzor hýbe, akou rýchlosťou, prestávky - neaktivita)
- Kliknutia (koľko a kde)
- Kedy stránku opustíme alebo obnovíme (vrátane prekliknutia na inú kartu v prehliadači)
- Scrollovanie a kde na stránke sa nachádzame
- Informácie o našom zariadení

Tieto dáta môžu byť využité mnohými spôsobmi – od uľahčenia, či personalizácie zážitku, zlepšenie bezpečnosti, až po cielenie reklám. Niektoré cookies teda benefitujú nás ako používateľov, niektoré benefitujú firmy a spoločnosti.

Najbežnejšie druhy cookies:

1. **Základné (nevyhnutné) cookies**: tieto cookies sú nevyhnutné pre základnú funkčnosť webových stránok. Ukladajú si informácie o tom, kto sme, takže sa nemusíme znovu prihlasovať vždy, keď stránku navštívime. Sú tiež zodpovedné za fungovanie košíka v e-shopoch. Tieto cookies nesmú byť vypnuté, pretože bez nich by stránky nefungovali správne.

2. **Funkčné cookies**: tieto cookies si pamätajú naše voľby a preferencie, ako napríklad jazyk, ktorým chceme stránku zobrazovať, alebo či chceme zobraziť tmavý alebo svetlý režim. Pomáhajú nám zlepšiť náš používateľský zážitok.

3. **Analytické cookies**: Analytické cookies zbierajú informácie o tom, ako používame stránku. Ukladajú informácie o tom, ktoré podstránky navštívime (konkrétny produkt v e-shope), ako dlho na nich zostaneme, a aké odkazy klikáme. Tieto údaje sú často anonymizované - použité ako štatistiky vytvorené z celých súborov dát. Slúžia na vylepšovanie stránok na základe toho, ako ich používme všetci - napr. či sú ikony správne rozmiestnené, aby bola pre používateľov stránka prehľadná.

4. **Cookies tretích strán (sledovacie cookies)**: tieto cookies sú najkontroverznejšie, pretože ich používajú tretie strany na sledovanie našej aktivity naprieč inými webovými stránkami. Často sa teda využívajú na cielenie reklám a sledovanie našich preferencií mimo pôvodnej stránky, ktorú ste navštívili. Tieto cookies môžu byť umiestnené reklamnými sieťami, ako je Google alebo Facebook, aby sledovali vašu aktivitu na internete a poskytovali reklamy založené na vašich záujmoch.

Čím viac údajov o vás webové stránky zbierajú, tým lepšie dokážu prispôsobiť obsah, ktorý vám zobrazujú. No zároveň to znamená, že veľká časť vášho správania na internete je podrobne monitorovaná a využívaná na marketingové a komerčné účely.

Cookies a GDPR (Všeobecné nariadenie o ochrane údajov)

Európska únia zaviedla v roku 2016 nariadenie GDPR, ktoré stanovuje pravidlá pre ochranu osobných údajov používateľov v online prostredí. Webové stránky musia teraz získať náš **informovaný súhlas** skôr, ako začnú zbierať cookies, a musia nás informovať o tom, aké údaje zbierajú a na aké účely. Práva podľa GDPR:

- **Právo na informácie**: Musíme byť informovaní o tom, aké cookies webová stránka používa a prečo.
- **Právo na odmietnutie**: Môžeme odmietnuť niektoré alebo všetky cookies, najmä tie, ktoré nesúvisia s nevyhnutným fungovaním stránky.
- **Právo na prístup k údajom**: Môžeme požiadať o prístup k údajom, ktoré webová stránka o nás zbiera prostredníctvom cookies.

Ako sa vyhnúť nástrahám a efektívne využívať cookies vo svoj prospech

Tým, že budeme aktívne spravovať cookies a vedome si vyberať, ktoré povolíme, môžeme využívať všetky výhody personalizácie a plynulého používania stránok, no zároveň minimalizovať riziká spojené so sledovaním našej online aktivity.

- **Odmietnite cookies tretích strán:** Cookies tretích strán sledujú našu aktivitu naprieč rôznymi stránkami, čo umožňuje spoločnostiam vytvárať komplexné profily o našom správaní a záujmoch. Tieto cookies sú často využívané na cielenú reklamu, ale môžu narušiť naše súkromie. Väčšina moderných prehliadačov umožňuje blokovať cookies tretích strán. Môžete ísť do nastavení prehliadača a vypnúť ich. Týmto krokom znížite množstvo dát, ktoré môžu spoločnosti o vás zbierať na reklamné účely.

- **Priebežne spravujte svoje cookies a nepotrebné mažte**: Cookies môžu byť zložité na správu manuálne, najmä ak často navštevujeme rôzne stránky. Existujú nástroje a rozšírenia, ktoré nám pomôžu spravovať cookies automaticky. Niektoré rozšírenia, ako napríklad **Cookie AutoDelete** (pre prehliadače Chrome, Firefox, Edge, či Brave), alebo aplikácie, napr. **Cookie** (pre operačný systém Mac OS), nám umožnia nastaviť, ktoré cookies chceme nechať aktívne a ktoré sa majú automaticky vymazať po odchode zo stránky. Stačí si nainštalovať aplikáciu alebo rozšírenie do svojho prehliadača, nastaviť svoje preferencie, a automatický systém bude sám mazať nepotrebné cookies.

Metadáta - Svet, ktorý nás počúva: Ako technológie poznajú naše zvyky

V tejto časti sa zameriame na metadáta, neviditeľné informácie, ktoré sa generujú našimi online a offline aktivitami. Rozoberieme, čo presne metadáta sú, ako vznikajú a aký majú význam v našom každodennom živote. Ukážeme si, ako technológie dokážu analyzovať naše správanie, zvyky a preferencie na základe údajov, ktoré sa zhromažďujú z rôznych zariadení. Na konkrétnych príkladoch si priblížime, aké typy metadát sú generované a ako tieto informácie ovplyvňujú náš digitálny a fyzický svet.

Náš online život, ba dokonca aj ten fyzický, generuje obrovské množstvo dát – tzv. metadát. Tieto neviditeľné informácie, ktoré sa zbierajú z našich zariadení, nám umožňujú komfort, personalizované zážitky, ale tiež odhaľujú, že technológie „poznajú“ naše zvyky oveľa lepšie, ako by sme si mysleli. V nasledujúcej kapitole si podrobnejšie vysvetlíme, čo presne metadáta predstavujú, akým spôsobom sa generujú a prečo sú tak dôležité v dnešnej digitálnej dobe. Zároveň si uvedieme konkrétne príklady rôznych typov metadát, ktoré technológie dokážu zbierať – od informácií o našej polohe, zvykoch a čase, ktorý trávime online, až po naše preferencie v oblasti médií, nákupov či dokonca sociálnych interakcií.

*Dve kamarátky, **Jana** a **Petra**, sa stretli v svojej obľúbenej kaviarni, ako každý piatok. Petra sa tam ponáhľala rovno z fitka, stále v športovom oblečení, s ružovými lícami a rozžiarenými očami po náročnom tréningu. Jana si to však ani nevšimla. Práve dobehla z práce s myšlienkami na posledný e-mail, ktorý musela odoslať, a bola pripravená si konečne oddýchnuť pri šálke kávy.*

Objednali si cappuccino a sadli si k stolu v rohu, vedľa okna. Petra, stále plná energie, začala rozprávať o svojich najnovších objavoch. „Jani, počúvaj, asi si kúpim ten Fit'o'clock nakoniec. Lebo chcem, aby mali moje fitness hodinky senzor srdcovej frekvencie aktívny neustále, aby som vedela presnejšie, koľko kalórií spálim. Tento aktuálny mi to odmeria, ale len keď kliknem na 'zmerať tep' a hneď potom zase prestane tep merať, takže nie je veľmi presný."

Jana Petru aktívne počúvala, aj keď sa do tejto témy veľmi neangažovala. „Akože, Peti, hrozne ťa obdivujem. Ale toto by som nedala. Strašne veľa roboty v poslednej dobe. Ale ja aj tak asi radšej precvičujem mozog, než zvyšok tela," usmiala sa.

*Keď sa obe rozlúčili, Jana sa pobrala domov. Bola unavená, a tak si po príchode ľahla na gauč a otvorila svoj mobil, aby si prešla sociálne siete a trochu si oddýchla. Ako si prezerala feed, zrazu si všimla niečo zvláštne. Medzi bežnými príspevkami sa začali objavovať reklamy na **fitness náramky**. „Čo to má byť?" zamračila sa. „Ja som o týchto veciach nikdy nič nevyhľadávala."*

Zrazu jej to prišlo podozrivé. Mala pocit, akoby ju jej telefón sledoval. Ako to, že jej mobil ponúka reklamy na niečo, o čom sa rozprávala len v kaviarni? „Určite ma to odpočúva," pomyslela si.

Čo však Jana nevedela, bol fakt, že mobily nepotrebujú odpočúvať naše rozhovory, aby o nás pomocou kombinácie údajov vydedukovať rôzne skutočnosti. Algoritmy, ktoré sú súčasťou aplikácií, pracujú na pozadí oveľa sofistikovanejším spôsobom. Petra si len pred hodinou prezerala podobné produkty na sociálnych sieťach a aktívne s nimi interagovala. Algoritmus si všimol, že obidve kamarátky zdieľali

rovnaké GPS súradnice, keďže sa stretli v tej istej kaviarni, ktorá bola priamo pod fitness centrom. Petra, ako pravidelná návštevníčka fitka, už mala „profil“ záujmov, ktorý zahrňoval fitness a zdravie, a keďže bola blízko Jany v tom istom čase, algoritmus usúdil, že aj Jana by mohla mať záujem o podobný produkt.

Čo sú metadáta?

Metadáta sú dáta o dátach. Zhromažďujú informácie o tom, ako používame naše zariadenia a internetové služby. Prepojené zariadenia dokonca medzi sebou zdieľajú dáta o svojom používateľovi a spoločne dokážu vytvoriť ešte presnejší profil. Čím viac máme prepojených zariadení, tým viac dokážu o nás vydedukovať.

Pokročilé dedukcie zariadení na základe metadát:

- Zariadenie môže napríklad rozpoznať, že jazdíme na elektrickej kolobežke - keď pedometer nezaznamenal kroky, zmena polohy v GPS neprebiehala tak rýchlo, ako zvyčajne prebieha pri cestovaní autom, GPS nezaznamenala priebežné zastavovanie, ako pri cestovaní autobusom, alebo električkou a senzor srdcovej frekvencie nezaznamenal fyzickú aktivitu, ako pri jazde na bicykli.
- Či pracujeme doobedia, na smeny, z domu, alebo nepravidelne - podľa toho, kedy chodievame spať a kedy vstávame môže zariadenie rozpoznať, či sme ranné vtáča, alebo nočná sova, ale aj kedy pracujeme.
- Aký je náš obľúbený žáner hudby, seriálov, kníh a podobne - stačí si pustiť zopár pesničiek, alebo filmov na streamovacích platformách a algoritmus podľa priradených označení vyhodnotí naše preferencie. Skutočne nám potom môže odporúčať tituly, ktoré nás oslovia viac, ako tituly náhodného výberu. Ale môže nám na podobnom základe odporúčať aj reklamy na podujatia, ako koncert, či premietanie v kine.
- Kedy máme najväčšiu tendenciu nepripravovať si jedlo sami, ale objednať si ho - algoritmus môže napríklad vyhodnotiť, že väčšina dní, kedy sme si spravili objednávku jedla, sú sviatky, alebo pravidelne vždy začiatkom mesiaca, lebo napríklad vtedy mávame svoje dni a počas nich máme viac apetítu a zároveň menej energie na prípravu jedla
- Zariadenie môže rozpoznať, že preferujeme pivo oproti vínu, podľa toho, že sme navštívili tri lokality označené ako pivárne, ale žiadnu vináreň.
- Zariadenie nám môže vytvoriť fotoalbum Dovolenka, kam vyberie fotografie z našej galérie, ktoré sme vytvorili počas daného časového úseku v oblasti mimo miesta. kde sa bežne zdržujeme (domáce prostredie), alebo fotoalbum Autoportréty, kde algoritmus vyberie fotografie, na ktorých rozpozná našu vlastnú tvár.
- Podľa obchodov, ktoré navštevujeme, vie mobil, produkty akých cenových kategórií preferujeme - lacnejšie značky, alebo luxusné obchody.
- Zariadenie môže dedukovať aspekty našej osobnosti, napríklad otvorenosť. Ak často skúšame nové reštaurácie, produkty alebo destinácie, algoritmus môže dedukovať, že sme otvorení novým zážitkom a inováciám.
- Naša politická orientácia - na základe čítania politických článkov alebo interakcií na sociálnych sieťach.

Keď tieto príklady zovšeobecníme, zistíme, že zariadenia majú celkom komplexný prehľad o mnohých stránkach našich životov. Základné zhrnutie oblastí dát, ktoré zariadenia zbierajú a vyhodnocujú:

- Naše základné biografické údaje (pohlavie, vek, bydlisko, vzdelanie, práca,...)
- Denné a spánkové návyky
- Poloha a pohybové vzorce
- Pracovné a produktívne návyky
- Zdravie a fitness aktivity
- Finančné správanie, nákupné zvyky a preferencie
- Dopravné návyky
- Záujmy a voľnočasové aktivity
- Sociálne interakcie a komunikácia
- Stravovacie a gastronomické preferencie
- Kultúrne a spoločenské aktivity
- Cestovné zvyky a preferencie
- Technologické preferencie a používanie zariadení
- Spotrebiteľské správanie, reklamné interakcie a citlivosť na zľavy
- Životný štýl a hodnoty
- Politické a spoločenské záujmy
- Osobnostné charakteristiky

Metadáta úzko súvisia s cookies. Operačné systémy a aplikácie dokážu na základe kombinácie dát o nás vyhodnotiť mnoho údajov, ktoré naše zariadenia následne uchovávajú. Preto je premýšľanie o tom, aké cookies stránkam odsúhlasujeme - aké informácie im o sebe poskytneme, tak dôležité.

Čo nám hrozí v online priestore

V tejto časti sa zaoberáme hrozbami, ktorým čelíme v online prostredí, pričom osobitnú pozornosť venujeme phishingu – jednej z najrozšírenejších techník kybernetických útokov. S každým kliknutím na odkaz alebo otvorením e-mailu sa môžeme vystaviť nebezpečenstvu straty osobných údajov či narušeniu finančnej bezpečnosti. Na konkrétnych príkladoch si ukážeme, ako phishingové útoky fungujú, aké triky útočníci používajú, aby nás oklamali, a ako sa im efektívne brániť.

V dnešnom digitálnom svete, kde sú naše osobné údaje stále cennejšie, čelíme mnohým rizikám a hrozbám v online priestore. S každým kliknutím, prihlásením či otvorením e-mailu sa môžeme vystaviť nebezpečenstvám, ktoré sú často nenápadné, no o to zákernejšie. Táto kapitola sa bude venovať jednej z najrozšírenejších techník hrozieb v online priestore – phishing-u, ktorý využíva našu nepozornosť a nedostatok ostražitosti, aby nás donútil k akcii, ktorá môže spôsobiť napríklad únik osobných údajov či narušiť našu finančnú bezpečnosť. Ukážeme si, ako tieto útoky prebiehajú, ako ich rozpoznať a ako sa pred nimi účinne chrániť.

Pozor na phishing.

Tomáš, mladý marketér, mal práve rušný deň v práci, keď mu prišla e-mailová správa. V predmete bolo veľkými písmenami napísané: "URGENT: Váš účet bol zablokovaný!". Bez veľkého premýšľania klikol na e-mail od jeho banky. V správe sa písalo, že jeho bankový účet bol napadnutý a aby ho odblokoval, musí okamžite kliknúť na odkaz a zadať svoje prihlasovacie údaje.

Tomáš cítil v žalúdku nepríjemné pnutie. Myšlienky mu vírili hlavou. "Čo ak mám naozaj zablokovaný účet? Ako zaplatím účty? Musím to vyriešiť hneď!" Bez toho, aby sa zamyslel nad podozrivosťou celej situácie, bol pripravený zadať svoje prihlasovacie meno a heslo.

*Na poslednú chvíľu mu však napadlo, že niečo nie je v poriadku. „Prečo mi banka posiela takú urgentnú správu e-mailom, keď zvyknú komunikovať prostredníctvom aplikácie?“ Tomáš sa pozrel bližšie na e-mailovú adresu odosielateľa a všimol si niečo divné: namiesto oficiálnej domény banky **bankaOK.sk** mu prišiel e-mail od **banka0K.sk**. „To nie je moja banka!“ uvedomil si so šokom.*

Rýchlo zavrel stránku a pre istotu zavolal priamo do banky. Po krátkom rozhovore mu potvrdili, že jeho účet je v poriadku a že išlo o phishingový pokus.

Phishing je **podvodná technika**, pri ktorej útočníci posielajú falošné e-maily, správy alebo vytvárajú webové stránky, ktoré sa tvária ako dôveryhodné, aby od používateľov **získali citlivé údaje, ako sú heslá, čísla kreditných kariet alebo prístupové kódy**. Tieto správy často obsahujú urgentné výzvy na akciu, ako napríklad tvrdenie, že náš účet bol ohrozený a musíme okamžite zadať svoje údaje na potvrdenie identity.

Phishingové útoky sú čoraz sofistikovanejšie a často využívajú vizuálnu podobnosť s oficiálnymi stránkami a logami dôveryhodných spoločností. Najlepší spôsob, ako sa chrániť pred phishingom, je byť opatrný/á pri otváraní neznámych e-mailov, neklikať na podozrivé odkazy a vždy si overiť autenticitu správ.

Rozpoznať phishing môže byť náročné, pretože útočníci sa snažia, aby ich správy vyzerali čo najdôveryhodnejšie. Existuje však niekoľko znakov, na ktoré si treba dávať pozor:

- **E-mailová adresa odosielateľa -** Odosielateľ sa môže tváriť, že ide o skutočného, dôveryhodného obchodníka, dokonca e-mailová adresa môže vyzerať ako autentická, ale keď sa na ňu lepšie pozrieme, zistíme, že má napríklad vymenené písmeno za iný podobný znak, čo máme bežne tendenciu prehliadnuť.
- **Apel na rýchlosť -** Phishingové správy často obsahujú urgenciu, ako napríklad výzvu, že musíme okamžite aktualizovať svoje údaje inak bude náš účet zrušený. Tieto správy sú navrhnuté tak, aby vyvolali paniku a primäli nás konať rýchlo.
- **Gramatické a pravopisné chyby -** Dôveryhodné firmy zvyčajne kontrolujú, aby ich komunikácia bola bezchybná. Ak si všimneme množstvo chýb v gramatike a pravopise, je to jasný varovný signál, že správa nie je legitímna. Väčšinou ide o nekvalitný preklad z iných jazykov pomocou dostupných online prekladačov.
- **Podozrivé odkazy -** Vždy skontrolujme, kam nás odkaz, na ktorý sa chystáme kliknúť, v skutočnosti zavedie, umiestnením kurzoru myši na odkaz **bez klikania**. Ak adresa nezodpovedá oficiálnej stránke, je lepšie naň neklikať.
- **Žiadosti o osobné údaje -** Legitímne spoločnosti nikdy nepožiadajú o citlivé údaje, ako sú heslá, čísla kreditných kariet alebo kódy cez e-mail alebo SMS. Ak správa vyžaduje tieto informácie, ide o phishingový pokus. Najvhodnejšie je vždy sa obrátiť na samotnú spoločnosť nejakým iným komunikačným prostriedkom.
- **Prílohy v správach -** Phishingové e-maily môžu obsahovať prílohy, ktoré sú škodlivé. Keď dostaneme nevyžiadaný e-mail s prílohou (najmä ak je to súbor typu .zip, .exe alebo iný spustiteľný súbor), nemali by sme ho otvárať.

Ak máte chuť sa otestovať, spravte si phishingový test, v ktorom si môžete vyskúšať či dokážete odhaliť podvodnú phishingovú správu. Pre zobrazenie výsledku testu, je potrebné prejsť všetkými 15 ukážkami emailov. Vyskúšať si to môžete so žiakmi.

Bezpečné heslo

V tejto časti sa zameriame na kľúčovú tému bezpečnosti – tvorbu a správu hesiel, ktoré sú našou prvou obranou proti kybernetickým hrozbám. Ukážeme si najčastejšie chyby, ktorých sa používatelia dopúšťajú pri vytváraní hesiel a poukážeme na riziká spojené s ich neadekvátnym uchovávaním. Ďalej si predstavíme efektívne metódy na vytváranie silných a unikátnych hesiel, pričom osobitnú pozornosť venujeme Schneierovej metóde, ktorá kombinuje zapamätateľnosť s vysokou úrovňou zabezpečenia. Cieľom podkapitoly je poskytnúť nástroje a poznatky, ktoré pomôžu užívateľom chrániť svoje online účty a osobné informácie pred potenciálnymi útokmi.

Heslá sú bránou k našim osobným údajom, financiám a citlivým informáciám. Ich bezpečnosť je preto nevyhnutná, no mnoho ľudí stále robí chyby pri ich tvorbe. V tejto kapitole si preto ukážeme príklady najčastejších chýb, ktorých sa ľudia pri tvorbe hesiel dopúšťajú a naučíme sa, ako vytvoriť naozaj bezpečné heslo, ktoré bude odolné voči moderným útokom.

Najčastejšie chyby Slovákov pri tvorbe hesiel

Slováci majú v oblasti tvorby hesiel ešte dlhú cestu pred sebou. Často používajú kombinácie, ktoré by hacker prelomil skôr, než si stihneme spraviť kávu. Tieto heslá sú jednoduché a vychádzajú z ľahko dostupných informácií o používateľovi, čo výrazne zvyšuje riziko ich prelomenia. Toto sú najpoužívanejšie kombinácie a heslá používateľov účtov na stránkach so slovenskou koncovkou **.sk**:

1. **Jednoduché sekvencie čísel**: Heslá ako „123456“, „123456789“ alebo „111111“ patria k najčastejším. Hoci sú ľahko zapamätateľné, útočníci ich vyskúšajú ako prvé pri pokuse o prelomenie hesla.
2. **Slovo „heslo“ alebo jeho varianty**: Veľa Slovákov používa slovo „heslo“, „password“ alebo jednoduché variácie ako „heslo123“, čo je extrémne ľahko uhádnuteľné.
3. **Osobné údaje**: Heslá ako „Jano1985“, „Maria75“ mená - svoje, alebo svojich detí, či použitie dátumu narodenia v rôznych kombináciách sú veľmi časté. Takéto informácie sú často dostupné cez sociálne siete, čo znižuje ich bezpečnosť.
4. **Jednoduché slová a frázy**: Obľúbené športové tímy, názvy miest („Slovensko“, „Bratislava“) alebo jednoduché frázy ako „milujemfutbal“ sa často používajú, čo robí tieto heslá predvídateľnými.

Používanie takýchto jednoduchých hesiel môže spôsobiť, že naše účty budú zraniteľné voči hackerským útokom. Moderné útoky využívajú automatické programy na hádanie hesiel, ktoré skúšajú milióny kombinácií v priebehu sekúnd, a práve tieto jednoduché heslá sú často prelomené ako prvé.

Nebezpečenstvá spojené s ukladaním hesiel

Pri spravovaní hesiel sa mnohí ľudia spoliehajú na rôzne metódy uchovávania, avšak nie všetky z nich sú bezpečné. Ako online služby a účty pribúdajú, čelíme otázke, ako si zapamätať alebo bezpečne uložiť veľké množstvo hesiel. Nevhodné spôsoby uchovávania hesiel môžu byť vážnym bezpečnostným rizikom, pretože uľahčujú prístup útočníkom, ktorí by chceli zneužiť naše citlivé informácie.

1. Heslá napísané na lístočku

Uchovávanie hesiel napísaných na lístočku alebo papieri je bežná prax, najmä v kanceláriách alebo domácnostiach. Toto riešenie síce zaručuje, že si heslo zapamätáme, no zároveň je veľmi nebezpečné. Ak si napíšeme heslo na lístok a prilepíte ho na monitor, alebo ho jednoducho uložíme v šuflíku, ktokoľvek, kto má fyzický prístup k nášmu pracovnému priestoru, môže tieto heslá ľahko nájsť. Okrem toho, ak sa stratí alebo sa dostane do nesprávnych rúk, máme problém, pretože heslo je odhalené.

2. Heslá uložené v prehliadači

Mnohé internetové prehliadače ponúkajú možnosť uložiť si heslá pre rýchle prihlásenie na rôzne stránky. Táto možnosť je pohodlná, pretože šetrí čas pri prihlasovaní, ale zároveň prináša veľké riziká. Ak má niekto fyzický alebo vzdialený prístup k vášmu zariadeniu, môže ľahko získať prístup k uloženým heslám. Niektoré prehliadače síce poskytujú možnosť heslá chrániť hlavným heslom alebo biometrickými údajmi, ale ak táto ochrana nie je aktivovaná, údaje sú zraniteľné.

3. Správcovia hesiel

Správcovia hesiel sú o niečo bezpečnejšou alternatívou na uchovávanie hesiel, keďže umožňujú ukladať rôzne heslá v šifrovanej podobe, pričom na prístup do správcu potrebujete jedno hlavné heslo. Správcovia hesiel tiež ponúkajú generovanie silných a unikátnych hesiel pre rôzne účty, čím sa eliminuje potreba používať slabé alebo opakujúce sa heslá. Aj keď sú správcovia hesiel považovaní za bezpečnejší spôsob správy hesiel, stále je tu určité riziko.

4. Pamätanie hesiel len v hlave

Mnohí ľudia sa spoliehajú na to, že si heslá jednoducho zapamätajú. Toto môže byť bezpečnejšie než používanie lístočkov alebo ukladanie v prehliadači, ale je tu limit v tom, koľko rôznych a komplexných hesiel si dokážeme zapamätať. Navyše, často to vedie k používaniu rovnakého hesla pre viaceré účty, čo je mimoriadne nebezpečné. Ak útočníci prelomia jedno heslo, môžu ho použiť na prístup k viacerým účtom. Ale, čím viac rôznych hesiel máme, tým ťažšie je si ich všetky zapamätať, čo vedie k sklonu používať jednoduché alebo ľahko zapamätateľné kombinácie.

Problém: Veľa účtov, rôzne heslá

Každý používateľ má v súčasnosti množstvo online účtov – od e-mailu, cez sociálne siete, až po online bankovníctvo a e-shopy. Odporúča sa, aby každé heslo pre jednotlivý účet bolo unikátne, čo drasticky zvyšuje počet hesiel, ktoré si musíme pamätať. Používanie rovnakého hesla na viacerých účtoch je mimoriadne riskantné, pretože ak jedno z hesiel unikne, útočníci môžu získať prístup k viacerým účtom. Ako teda riešiť tento problém, keď sa odporúča mať na každom účte iné heslo a to by malo byť zároveň silné a bezpečné?

Riešením je používanie bezpečných metód na tvorbu hesiel, ktoré umožnia vytvoriť unikátne a silné heslá pre každý účet, pričom tieto heslá zostanú zapamätateľné.

Schneierova metóda: Ako si vytvoriť silné a zapamätateľné heslá

Jedným z najefektívnejších spôsobov, ako vytvoriť silné a zároveň zapamätateľné heslo, je **Schneierova metóda**, ktorú navrhol odborník na bezpečnosť Bruce Schneier. Táto metóda spočíva v transformácii jednoduchej vety na komplexné heslo, ktoré je pre používateľov ľahko zapamätateľné, no pre útočníkov mimoriadne ťažko prelomiteľné. Dokonca môžeme použiť aj mená a iné citlivé údaje, len ich musíme trochu zašifrovať.

Poďme si to vyskúšať - vytvorte si prvé heslo podľa Schneierovej metódy:

1. **Vyberte si náhodnú vetu, známy citát, alebo frázu, na ktorú nemáte šancu zabudnúť.**
   Vyberte si vetu, ktorá je vám známa, ale nie je úplne predvídateľná. Môže to byť citát z filmu, knihy, obľúbená pieseň alebo len jednoduchá osobná veta. Napríklad:
   „Neznášam pondelky.“

2. **Zmeňte niektoré písmená na špeciálne znaky a čísla, alebo pri dlhšej vete vezmite prvé písmená z každého slova vety a potom niektoré zmeňte na špeciálne znaky a čísla. Použite aspoň 12 znakov.**

“n3zn@s@mp0nd31ky”

3. **Pridajte ďalšie špeciálne znaky**
   “!!n3zn@s@m_p0nd31ky!!”

4. **Použite kombináciu malých a veľkých písmen**
   Pre ešte vyššiu bezpečnosť môžete použiť kombináciu malých a veľkých písmen, aby sa zvýšila zložitosť hesla.
   Finálne heslo môže vyzerať napríklad takto:
   „!!N3zn@s@M_p0nd31kY!!“

Prečo je Schneierova metóda účinná?

- **Jednoduchosť pre používateľa**: Hoci heslo vyzerá komplikovane, pre nás bude jednoduché na zapamätanie, pretože jeho základom je veta, výrok, či fráza, ktorú poznáme. Nie je potrebné si zapamätať náhodný sled znakov.
- **Zložitosť pre útočníkov**: Schneierova metóda vytvára heslá, ktoré sú náhodné a ťažko uhádnuteľné pre útočníkov, čo robí heslá silnejšími proti metódam ako sú slovníkové útoky alebo brute force útoky.
- **Flexibilita**: Schneierova metóda umožňuje prispôsobiť heslo podľa konkrétnych požiadaviek. Môžeme pridať viac znakov, špeciálne symboly alebo rôzne kombinácie, čím kombinujeme jednoduchosť na zapamätanie s vysokou bezpečnosťou.

10 tipov pre bezpečné online nakupovanie:

1. Používajte len zabezpečené stránky (HTTPS)

- Skontrolujte, či webová stránka používa protokol **HTTPS** (Hypertext Transfer Protocol Secure), čo indikuje šifrované spojenie medzi vaším zariadením a serverom. Adresa URL by mala začínať „https://“ a mala by byť doplnená o ikonu zámku vedľa adresného riadku.
- **Prečo je to dôležité?**: HTTPS zabezpečuje, že vaše osobné údaje a platobné informácie budú šifrované a chránené.

2. Vyhýbajte sa verejnej Wi-Fi pri online platbách

- Nikdy nevykonávajte online platby alebo nezadávajte citlivé údaje cez verejné Wi-Fi siete, ktoré nie sú dostatočne zabezpečené. Použite **mobilné dáta** alebo zabezpečenú súkromnú Wi-Fi sieť.
- **Prečo je to dôležité?**: Verejné Wi-Fi siete sú náchylné na útoky, pretože nie sú šifrované a útočníci môžu ľahko zachytiť vaše osobné údaje.

3. Pozor na príliš dobré ponuky

- Ak ceny vyzerajú až príliš lákavo alebo sú výrazne nižšie ako obvyklé trhové ceny, môže ísť o podvod. Vyhnite sa stránkam s extrémne lacnými ponukami bez overenej histórie.
- **Prečo je to dôležité?**: Podvodníci často lákajú na nereálne ponuky, aby získali údaje od nič netušiacich zákazníkov.

4. Používajte jednorazové platobné karty alebo virtuálne karty

- Niektoré banky a služby ponúkajú možnosť vytvoriť **jednorazovú virtuálnu platobnú kartu**, ktorá sa dá použiť len raz alebo na obmedzený čas.
- **Prečo je to dôležité?**: Znižuje to riziko, že vaše hlavné kreditné karty budú napadnuté, ak dôjde k úniku údajov.

5. Sledujte svoje transakcie

- Pravidelne kontrolujte svoje bankové výpisy a online transakcie, aby ste si všimli akékoľvek podozrivé alebo neautorizované platby.
- **Prečo je to dôležité?**: Včasná identifikácia podvodných transakcií vám umožní rýchlejšie reagovať a minimalizovať straty.

6. Skontrolujte obchodné podmienky e-shopu

- Predtým, než uskutočníte nákup - uzavriete zmluvu s e-shopom, najskôr si preverte, či v obchodných podmienkach nečíhajú nejaké drobné písmenká znevýhodňujúce spotrebiteľa, ak e-shop funguje právnou formou s.r.o, preverte firmu na finstat.sk.
- **Prečo je to dôležité?**: Zásady ochrany súkromia vám ukážu, či je stránka dôveryhodná a či sú vaše údaje chránené pred zneužitím.

7. Vypínajte ukladanie platobných údajov

- Mnohé stránky ponúkajú možnosť **uložiť platobné údaje** na budúce nákupy. Ak to nie je nevyhnutné, túto funkciu nepoužívajte.
- **Prečo je to dôležité?**: Uložené údaje môžu byť zneužité, ak dôjde k úniku údajov alebo napadnutiu stránky.

8. Používajte antivírus a firewall

- Nezabúdajte na používanie **antivírusového softvéru a firewallu**, aby ste ochránili svoje zariadenie pred malvérom a neoprávneným prístupom.
- **Prečo je to dôležité?**: Malvér a phishingové útoky môžu ukradnúť vaše osobné údaje alebo poškodiť váš systém.

9. Pred nákupom kontrolujte recenzie

- Skontrolujte, či má stránka alebo produkt **prirodzene vyzerajúce recenzie**. Ak sú všetky recenzie pozitívne alebo veľmi podobné, môže ísť o falošné recenzie.
- **Prečo je to dôležité?**: Falošné recenzie sú častou taktikou podvodných e-shopov na vytváranie dojmu dôveryhodnosti.

10. Kontrolujte certifikáty stránok

- Kliknite na ikonu zámku v URL riadku, aby ste si overili, či má stránka **platný certifikát SSL** (Secure Socket Layer). Ak certifikát chýba alebo je neplatný, stránka nie je dostatočne zabezpečená.
- **Prečo je to dôležité?**: Certifikát SSL zaručuje, že vaša komunikácia so stránkou je šifrovaná a chránená pred odpočúvaním.

Cvičenie: Ako skontrolovať zabezpečenie webovej stránky

1. **Otvorte svoj prehliadač** (napr. Chrome, Firefox, Safari atď.).
2. **Navštívte ľubovoľnú webovú stránku**.
3. Skontrolujte ikonu na ľavej strane adresného riadku: Kliknutím na ikonu vedľa adresy môžete získať podrobné informácie o súkromí, súboroch cookie, nastaveniach webu a ďalších údajoch týkajúcich sa webovej stránky.

Niektoré prehliadače umožňujú ďalšie nastavenia na zlepšenie bezpečnosti - **Vždy používať zabezpečené pripojenia**. Aktivovaním tejto funkcie vás prehliadač upozorní pred tým, ako sa pripojíte k stránke, ktorá nepodporuje HTTPS. Ak stránka nie je zabezpečená, zobrazí sa varovanie, že pripojenie nie je bezpečné.