

Kybernetická bezpečnosť

16.10.2024

TUKE



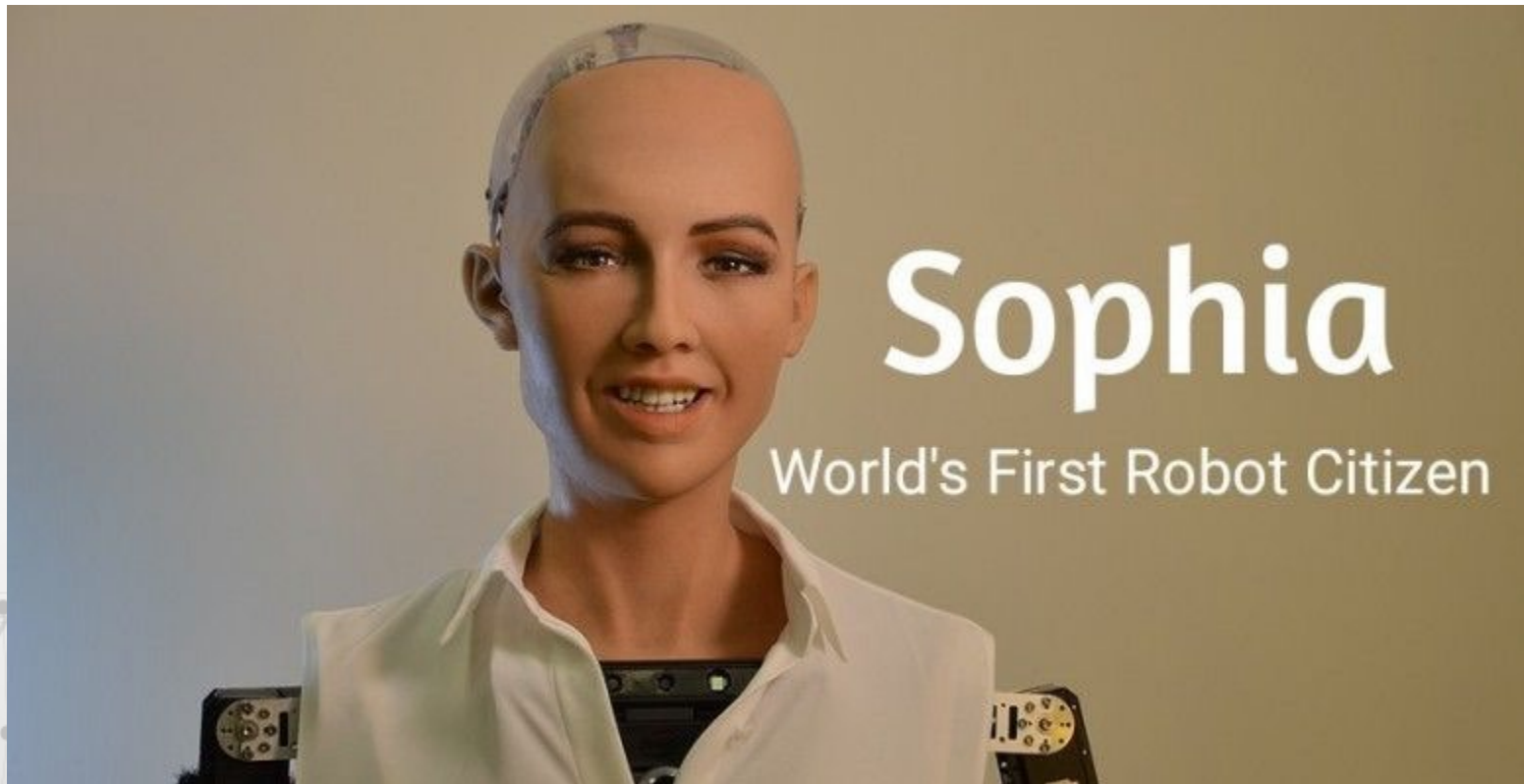
Ing. Peter Matej
matej.peter@emsec.sk

Bezpečnostné hrozby okolo nás

Kde „začína“ KB?



Človek alebo robot?



February 28, 2018

On Tuesday, February 27, Century College and the White Bear Area Chamber of Commerce, in conjunction with Hanson Robotics, LTD, hosted a special luncheon meeting featuring Sophia, the latest and most advanced humanoid robot.

AI – predpovede na rok 2024

- LLM ako triediaci nástroj ukradnutých dát
- AI ako analytický nástroj pre výber cieľa hackerského útoku
- AI ako nástroj zberu citlivých dát pri „neschválených“ použitíach
- Tvorba cielených phishingových a malvérových útokov
- Nárast škodlivých AI nástrojov ako WormGPT, FraudGPT
- Postupný presun LLM nástrojov z cloud do EndPoint, nové zranit.
- Malvér šitý na mieru
- Automatizácia útokov nie len v IT, ale aj v OT svete
- Nárast dezinformačných kampaní
- Deepfake

ENISA – predikcie do 2030

TOP 10 EMERGING CYBER- SECURITY THREATS FOR 2030



Zdroj: <https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030>

Každodenné nástrahy



- Free WiFi – naskenujte si QR kód!
- Na pošte vás čaká balík – doplaťte 2,69.-€
- Banka vám pozastavuje platnosť karty, na obnovenie kliknite [sem](#)
- [Splň túto úlohu a pridáme si ťa do skupiny!](#) (hrozba pre deti)
- iPhone (čokoľvek) posledný model za ¼ ceny, len dnes! [Registruj sa!](#)
- Tu licenčné centrum Microsoft, zistili sme nezrovnalosti, budeme vás navigovať pri oprave ...
- Ušetríte a [stiahnite si zadarmo SW](#) na domáce použitie
- Funkčný crack na drahý SW!
- Stiahni si [film zadarmo](#)
- 128 GB USB kľúč na zemi? Toľko šťastia!
- Máme tvoje intímne foto/video, zaplať, lebo...!
- Vieme, že Ťa podvádza partner, tu máš dôkazy (mail, QR ...)

Neznámy telefonát

- Nečakané zahraničné telef. číslo

- +420234234302

- <https://www.vyhledatcislo.cz/>

- <https://www.neznamecislo.sk/>

- Nečakané Slovenské telef. číslo

- Spoofing telefónnych čísel je realita

Príklad:

<https://www.imyfone.com/change-location/best-call-spoof-app/>

Neznámy telefonát – možný priebeh

- Anglický hlas na slovenskom čísle
- Hrozba väzením
- „Push 1“ to talk with police officer



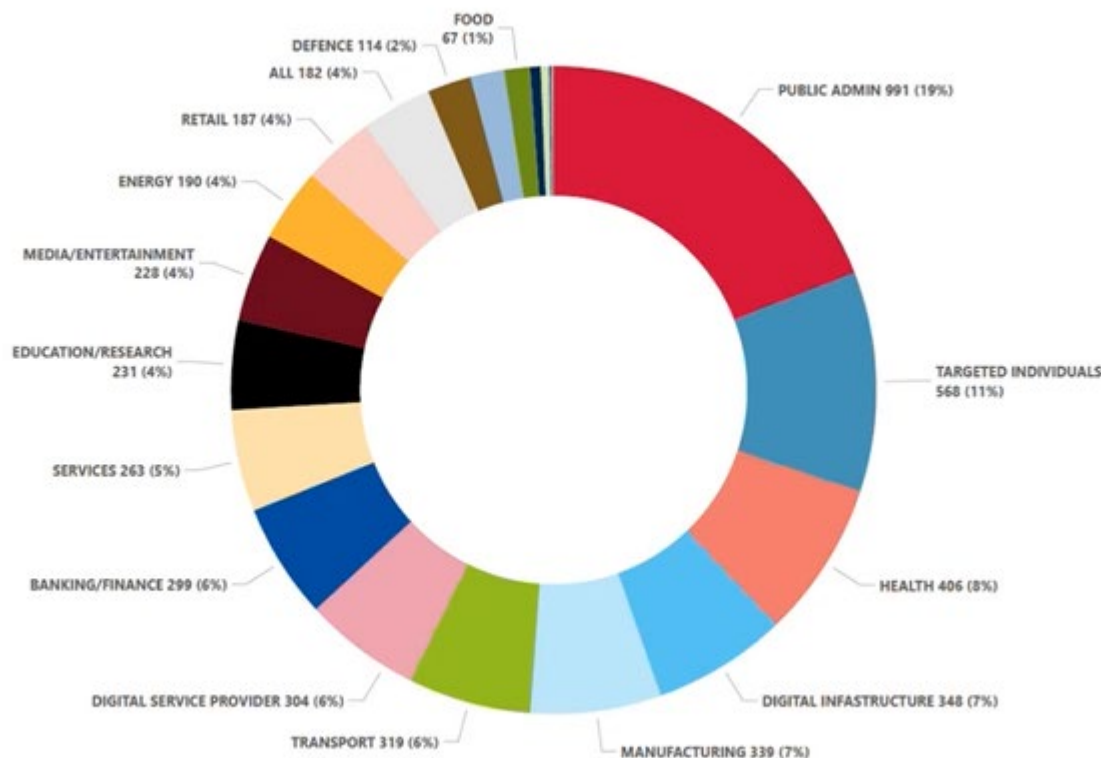
Neznámy telefonát – možný dopad

- Zmena účtovania tarify
- Prezradenie osobných identifikačných údajov
- Stresové bankové prevody a iné finančné konania
 - Príklad z SK: podvedená pani 3 prevody – spolu 1500.-€



Jednotlivec ako cieľ útoku?

- cieľové sektory, júl 2022 – jún 2023



<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>

Fyzická a digitálna identita

- Digitálna identita a digitálne zdravie, digitálna hygiena
 - Aké máme digitálne návyky? (fyzická identita vs. digitálna identita)
 - Ako vnímame kybernetickú bezpečnosť doma, v škole, v práci, v reštaurácii, v hoteli...?
 - Koho sa týka zákon č. 69/2018 Z. z.? A čo „ovplyvňuje“ ostatných?
- Aké dôležité sú bezpečnostné témy z oblasti „osobnej“ KB?
 - Existujú jasne vymedzené hranice?
 - Ovplyvňuje naše bezpečnostné správanie sa doma bezpečnosť organizácie/školy?
 - Ja budem právnikom, lekárom, xyz, ja KB NEPOTREBUJEM!!! **Či?**

Koľko stojí naša (digitálna) identita

- Kreditná karta so zostatkom do 5000 usd/eur - **\$110**
- Kreditné karty vrátane CVV - **\$20 až \$30**
- Klonovaná VISA/Mastercard/AE karta s pinom - **\$20**
- Heknutý Facebook/Instagram účet - **\$20**
- Heknutý Gmail účet - **\$60**
- Netflix, ročné predplatné - **\$20**
- Spotify účet - **\$10**
- Scany pasov a vodičákov – **\$20 až \$110 (USA)**
- Pas viacerých EU krajín (fyzický dokument) - **\$3000**
- Zdravotné údaje (zdravotná karta) \$40- \$100
 - <https://www.privacyaffairs.com/dark-web-price-index-2023/>

Odkiaľ „berie“ Dark Net osobné údaje?

';--have i been pwned?

Check if your email address is in a data breach

email address pwned?

Using Have I Been Pwned is subject to [the terms of use](#)

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

[Why 1Password?](#)

744	12,961,127,682	115,769	228,884,627
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

	772,904,991 Collection #1 accounts
	763,117,241 Verifications.io accounts
	711,477,622 Onliner Spambot accounts
	622,161,052 Data Enrichment Exposure From PDL Customer accounts
	593,427,119 Exploit.In accounts
	509,458,528 Facebook accounts

Recently added breaches

	207,114 Spoutible accounts
	5,970,416 MyPertamina accounts
	15,111,945 Trello accounts
	70,840,771 Naz.API accounts
	4,670,080 Hathway accounts
	3,869,181 Legendas.TV accounts
	48,145 DC Health Link accounts

<https://haveibeenpwned.com/>

Stav, keď zrejme máme problém

https://haveibeenpwned.com

Check if your email or phone is in a data breach

karinapalmer@orange.net

pwned?

Oh no — pwned!

Pwned in 5 data breaches and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com

CUV6U4!GU

29. január 2024 – 4. február 2024

The Week in Cyber Security and Data Privacy: 29 January – 4 February 2024

👤 Neil Ford 📅 6th February 2024

38,846,799 known records breached in 140 publicly disclosed incidents

Welcome to this week's global round-up of the biggest and most interesting news stories.

At the end of each month, these incidents – and any others that we find – will be used to inform our **monthly analysis of data breaches and cyber attacks**.

<https://www.itgovernance.co.uk/blog/the-week-in-cyber-security-and-data-privacy-29-january-4-february-2024>

„Osobné“ bezpečnostné hrozby

1. Sociálne inžinierstvo
2. Sociálne siete, ich využitie a zneužitie
3. Phishingové útoky
4. E-mail, e-shop, internet
5. Heslá a autentifikácia
6. Verejné WiFi
7. Prenosné média
8. Fyzická bezpečnosť
9. Bezpečnosť mobilných zariadení
10. Bezpečnosť domáceho prostredia
11. Home office a práca na diaľku

Sociálne inžinierstvo - taktiky



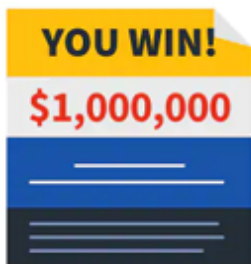
"Priateľ" pošle zvláštnu správu



Zvýšené emócie



Urgentná požiadavka



Ponuka je až príliš dobrá, aby bola pravdivá



Poskytnutá pomoc, ktorú ste nežiadali



Odosielateľ nevie potvrdiť svoju identitu

Sociálne inžinierstvo - taktiky

Príklad



INTERPOL-EUROPOL
Polícia pre počítačovú kriminalitu

POLÍCIA

PREDVOLANIE NA SÚD
Na účely súdneho vyšetrovania

EUROPOL A SLOVENSKÁ POLICAJNÁ JEDNOTKA NA OCHRANU DETÍ

Správa o vyšetrovaní počítačovej kriminality

(Článok 187-1 a 2 Trestného zákona)

Pozor!

Som plukovník Ľubomír Solák (Náčelník Polície). Spolupracujeme s europolom v boji proti počítačovej kriminalite.

Chceli by sme vás informovať, že sme iriadili komplexný systém dohľadu na nepretrhlé monitorovanie činnosti na digitálnych sieťach, ako sú pornografické stránky, rozpravacie služby a sociálne médiá.

Kontaktujeme vás na základe vyšetrovania našej kybernetickej spravodajskej jednotky, ktoré potvrdilo, že ste na internete spáchali kybernetický trestný čin (týkajúci sa detskej pornografie, pedofílie, exhibicionizmu a kybernetickej pornografie).

Radi by sme vás informovali, že ste boli obvinení z nasledujúcich trestných činov:

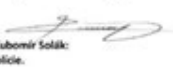
- * kybernetickej pornografie
- * šírenie pornografických obrázkov
- * detská pornografia
- * pedofília

Týmto vás žiadame, aby ste na tieto štyri obvinenia reagovali v prísne stanovenej lehote 48 hodín. Ak nebudete reagovať, budeme nútení vydať príkaz na zatknutie a zatknúť vás, pričom sa na vás budú vzťahovať (články 187-1 a 2 Trestného zákona Slovenskej republiky, ktoré zakazujú šírenie, držanie a prístup k detskej pornografii na internete. Za to hrozí trest odňatia slobody na päť rokov a pokuta 75 000 eur.

Upozorňujeme, že na tento e-mail je potrebné odpovedať okamžite.

S úctou,

Plukovník Ľubomír Solák:
Náčelník polície.





Europol je medzivládny orgán, ktorý uľahčuje výmenu informácií medzi národnými policajnými zložkami v EÚ a iných krajinách, terorizme, medzinárodnej trestnej činnosti a pedofílii. Euroapol funguje od roku 1999 a od roku 2000 je európskou agenciou financovanou z rozpočtu Spoločenstva, a preto podlieha kontrole Európskeho parlamentu.



POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY.

PREDVOLAJ NA SÚD
Na vyšetrovanie (článok 331-1-22 Trestného zákona)

Slovenská polícia v spojení s medzinárodnou políciou (INTERPOL). Kontaktuje vás krátko po zabavení počítača kybernetickej infiltrácie (oprávnenej vrátane detskej pornografie, pornografických stránok, kybernetickej pornografie, aby vás informoval, že ste predmetom niekoľkých právnych konaní, ktoré zahŕňajú:

VÝPOČTY POPLATKOV:

- *DETSKÁ PORNOGRAFIA.
- *PORNOGRAFICKÁ STRÁNKA.
- *CYBER PORNOGRAFIA.
- *NESPRAVNE VYUŽÍVANIE MALÝCH LÝCH.

Žiadame vás, aby ste sa vyjadrili e-mailom tak, že nám napíšete svoje odôvodnenia, aby sme ich preskúmali a skontrolovali, aby sa vyhodnotili sankcie; že v prísnom termíne 72 hodín. Po uplynutí tejto doby budeme povinní postúpiť naše oznámenie ktorémukoľvek prokurátorovi republiky v blízkosti súdu prvého stupňa a špecialistovi na počítačovú kriminalitu, aby na vás uvalil väzbu a budete zaregistrovaný ako sexuálny delikvent.

Teraz ste boli varovaní.



Sociálne inžinierstvo

- Hrozba:
 - Uvedenie človeka do nekomfortnej situácie, vyvolanie stresu, časového nátlaku, zodpovednosti za možné finančné straty. Najčastejšie na diaľku, telefonicky.
 - Vyžadovanie informácií o prístupoch do systémov (zmena prístupového hesla v dôsledku nefunkčnosti), informácie o konfigurácii, o procesoch v organizácii.
- Odporúčanie:
 - Neposkytovať informácie telefonicky „neznámym“ osobám v telefóne (banka, poisťovne, štátne organizácie a inštitúcie).
 - Vyžiadať si meno komunikujúceho, organizáciu, pozíciu. Nevolať na telefónne číslo, ktoré poskytne volajúci, volať na oficiálne čísla organizácie/inštitúcie.

Sociálne siete, využitie, zneužitie

- Hrozba
 - Zdroj informácií, ktoré je možné využiť pri sociálnom inžinierstve (fotky, statusy, CV, popis pracovnej pozície, činnosti, ale aj informácie o rodinnom zázemí).
 - Sociálne siete sú základným zdrojom pri **OSINT** metódach, bežným nástrojom HR pri vyhľadávaní a zamestnancov a výberových konaniach
 - Zdrojom pre analytické spoločnosti, ovplyvňovanie verejnej mienky a sociálnych nálad, zdrojom pre ovládanie (nielen) mladých ľudí a priestorom pre kyberšikanu.
- Odporúčanie
 - Minimalizovať poskytovanie verejných informácií
 - Pozor na verejné statusy a vyjadrenia (čo sa na internet dostane, to tam aj zostane!)

OSINT – „starší“ příklad



John McAfee  @officialmcafee · Jan 28

Yesterday on the way to London.

A free beer to anyone who can guess where we were.

Provided you are in London:)



Vydieranie na sociálnych sieťach

Vydieranie je trestný čin, ktorý zahŕňa použitie vyhrážok alebo násilia na získanie peňazí alebo majetku od niekoho. Na platformách sociálnych médií má vydieranie často podobu vydierania používateľov citlivými alebo kompromitujúcimi informáciami. Sexuálne vydieranie je na druhej strane špecifickým typom vydierania, ktoré zahŕňa vyhrážanie sa zverejnením sexuálne explicitného obsahu, pokiaľ obeť nespĺní požiadavky vydierača. Tieto činy môžu mať pre obete vážne osobné aj profesionálne následky.

Najčastejšie zneužívané platformy: Facebook, Instagram, Twitter/X, TikTok, WhatsApp, Ashley Madison, Snapchat

Ako reagovať?

- Zachovať pokoj a zdokumentovať dôkazy
- Zastaviť komunikáciu s vydieračom
- Nahlásiť incident platforme
- Poradiť sa s právnikom
- Obrátiť sa na orgány činné v trestnom konaní
- Posilniť ochranu súkromia
- Vzdelávať sa

„Nový“ fenomén – vyzliekacie aplikácie



Vľavo neexistujúca žena vytvorená nástrojom Midjourney. Na zábere vpravo ju „aplikácia na vyzliekanie“ za pár sekúnd vyzliekla. Je dodatočne upravená. Foto – Midjourney a DenníkN



Vydieranie mailom:

Od karinapalmer@orange.net

Odpovedať

Odoslať ďalej

Komu ja <emsec@emsec.sk>

Predmet **Máte nezaplatenú platbu. Vyžaduje sa úhrada dlhu.**

Dobrý deň,

Som hacker a úspešne som získal prístup do vášho operačného systému.
Mám tiež plný prístup k vášmu účtu.
Keď som sa nabúral do vášho ú

Sledujem vás už niekoľko mesiacov.

Skutočnosť je taká, že váš počítač bol infikovaný škodlivým softvérom prostredníctvom stránky pre dospelých, ktorú ste navštívili.
Ak s tým nie ste oboznámení, vysvetlím vám to.
Trojský vírus mi dáva plný prístup a kontrolu nad počítačom alebo iným zariadením.
To znamená, že môžem vidieť všetko na vašej obrazovke, zapnúť kameru a mikrofón, ale vy o tom neviete.
Mám tiež prístup ku všetkým vašim kontaktom a všetkej vašej korešpondencii.

Prečo váš antivírusový program nezistil škodlivý softvér?
Odpoveď: Malvér, ktorý som použil, je založený na ovládačoch, jeho signatúry aktualizujem každé 4 hodiny.
Preto váš antivírus nie je schopný zistiť jeho prítomnosť.
Vytvoril som video, na ktorom je vidieť, ako sa uspokojujete v ľavej polovici obrazovky,
a v pravej polovici je zobrazené video, ktoré ste v tom čase sledovali.

Jedným kliknutím myši môžem toto video poslať všetkým vašim e-mailom a kontaktom na sociálnych sieťach.
Môžem tiež zverejniť všetku vašu e-mailovú korešpondenciu a históriu chatu na messengeroch, ktoré používate.

Ak nechcete, aby sa to stalo, prevedte 1250€ v ekvivalente bitcoinu na moju bitcoinovú adresu
(ak neviete, ako to urobiť, stačí si vyhľadať "kúpiť bitcoin" na Googli).

Moja bitcoinová adresa (peňaženka BTC) je: **1Bd153BpyPYMHmaS4dQ4aZtAMedp4sonsT**

Phishing, Vhishing, Smishing

- Hrozba:

- Phishing – vyvolanie zdania výhodnosti, neodolateľnosti, akútnosti informácie, alebo konania
- Zvyčajne spolu s prvkami sociálneho inžinierstva
- Rôzne formy: phishing – mail s pripojeným dokumentom, alebo link/odkaz na zdroj informácie; vhishing – telefonát so zmeneným hlasom, smshing – podvodné SMS
- Doplnené deepfake videom! – Prípad GymBeam: zamestnanec spoločnosti 15 minút strávil na videohovore s „videokópiou“ šéfa GymBeam

- Odporúčanie:

- Nedôverovať neznámym odosielateľom, neklikáť na linky v mailoch, neotvárať vložené dokumenty, pokiaľ nie sú od dôveryhodnej osoby.
- Pokiaľ sa nám nepozdáva štylizácia mailu či správy, overiť si informáciu u odosielateľa (zákazník, partner, dodávateľ), môže ísť o únik identity.

Najčastejšie formy

- Falošná faktúra
- Zmena na E-mail účte
- Dodatočný poplatok za dopravu, clo, ...
- Odkaz na Google Docs
- Odkaz na platobný systém / banka
- Odkaz na uložený dokument – napr. dropbox
- Správa od verejnej inštitúcie
- Správa od služby (MS account, spotify ...)

Otestovanie linky? ÁNO. Web sandbox, napr. urlscan.io

Phishing, Vhishing, Smishing - príklady

Od Československa Obchodni Banka, A.S. <info@philcarter.it> 

Komu ja <emsec@emsec.sk> 

Predmet **ČSOB: (1) Dôležité nové upozornenie**

 Na ochranu vášho súkromia Thunderbird v tejto správe zablokoval vzdialený obsah

Vážený zákazník,

V schránke Československej obchodnej banky máte dôležitý list. Skontrolujte svoj e-mail kliknutím na:

Prosím, neignorujte túto správu, aby ste sa vyhli problémom v budúcnosti.

Zadajte zabezpečenú oblasť

Tieto pokyny boli zaslané všetkým klientom ČSOB a sú povinné okamžite vyhovieť.

Vďaka.
Československá obchodná banka, a.s.

ČSOB.

Neklikat' !

<https://neobution.de/wp-admin/sk3.php>

© ČSOB 2022

Phishing, Vhishing, Smishing - príklady

Od Websupport s.r.o. <websupport@sovatem.it> 

Komu ja <emsec@emsec.sk> 

Predmet **Predfaktúra 1022194625 [Websupport] (Pré-facture 1022194625 [Websupport])**

 Na ochranu vášho súkromia Thunderbird v tejto správe zablokoval vzdialený obsah

websupport

Stačí skontrolovať, uhradiť a je to

02.07.2022
Vystavenie predfaktúry

Vážený zákazník,

tešíme sa, že ste s nami. V prílohe vás čaká predfaktúra za objednané služby.
Overte svoje fakturačné údaje a zaplatte do 24 hodín. Po prijatí platby vám obratom pošleme originál faktúry a ak služby čakajú na spustenie, ihneď na tom začneme pracovať.

OBNOVIŤ MOJE PRODUKTY / ZAPLATIŤ ÚČTY

Vaša objednávka
Variabilný symbol faktúry: **1022194625**

Názov	Služba	Suma
Doménové meno	emsec.sk	13.99 EUR

Spolu na úhradu **13.99 EUR s DPH**

Neprajete si viac fakturovať niektorú z uvedených služieb? Jednoducho ju odstráňte [tu vo WebAdmine](#).

Skontrolujte si prosím fakturačné údaje

Jaroslav Chrupka IČO:
Jarná 38, 01001 Žilina DIČ:
SK IČ DPH:

Našli ste v údajoch chybu? Opravte ju jednoducho a pohodlne na [tomto linku](#).

Potrebujete pomôcť?
Volajte na (02) 20 60 80 80
alebo píšete na helpdesk@websupport.sk

Ako preverit' či URL (linka) je zlomyseľná?



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



Search or scan a URL

<https://www.virustotal.com>

E-mail, bazos, e-shop

- Hrozba

- Používanie rovnakého e-mailového účtu na firemné a súkromné účely
- Registrácia do rôznych aplikácií, portálov, služieb pomocou jediného e-mailového účtu
- E-shopy, bazáre a falošné reklamné kampane. Účel: zisk kontaktných údajov
- Internet: platforma pre novodobé vydieranie: zverejňovanie uniknutých osobných a firemných údajov

- Odporúčanie

- Oddelenie firemnej a súkromnej mailovej komunikácie
- Využitie viacerých mailových účtov pri registráciách do rôznych typov služieb
- Nepodľahnúť klamlivej reklame. „Nič nie je zadarmo.“ Ak je niečo podozrivo lacné, tak je to ozaj **podozrivo** lacné!
- Zverejňovať minimum osobných informácií pri registráciách. Overené e-shopy.

Ako nenaletieť pri predaji na bazos

- Hrozba
 - Prezradenie údajov o platobnej karte
 - Kupujúci pošle linku, kde treba zadať údaje o karte. Nezmysel!
 - Alebo napíše, že nefunguje platobné tlačítko, aby ste mu poslali mail
- Odporúčanie
 - Keď sa okamžite do pár minút ozve záujemca o tovar, nepodľahnúť radosti
 - Ak je to možné, skontrolovať hodnotenie predávajúceho
 - Nezdieľať svoje citlivé údaje. Na poslanie peňazí MUSÍ stačiť kupujúcemu vaše číslo účtu. Nepotrebuje číslo vašej karty!
 - Keď vám niekto „posiela peniaze“, nikdy nepotvrdzujte platbu! Platba sa potvrdzuje pri platení, nie keď vám niekto peniaze posiela.

Falošné e-shopy

- Hrozba
 - Prezradenie údajov o platobnej karte
 - Únik osobných údajov
 - Únik prihlasovacích údajov (ak máte všade rovnaký mail a heslo)
- Odporúčanie
 - Skontrolovať či má e-shop uvedené obchodné kontakty
 - Skontrolovať, či má e-shop obchodné podmienky
 - Či má recenzie, koľko a aké, pozrieť prípadne soi.sk (rizikové e-shopy)
 - Možnosti platby a doručenia (ak len platba vopred, asi je niečo zle)
 - **Pozor na neodolateľné ponuky, zľavy 90% a veci „zadarmo“**
 - mBank, Tatra banka – jednorázové platobné karty

Password or NOT Password



Počet znakov

Ako znaky „namiešať“

Ako heslo „vymyslieť“

Koľko hesiel používať?

Ako si ich pamätať?

Password or NOT Password

Počet znakov	Typ znakov	Iba číslice	Veľké, alebo malé písmená	Kombinácia veľkých a malých písmen	Čísla, veľké a malé písmená	Čísla, veľké a malé písmená, symboly
4		Okamžite	Okamžite	Okamžite	Okamžite	Okamžite
5		Okamžite	Okamžite	Okamžite	Okamžite	Okamžite
6		Okamžite	Okamžite	Okamžite	Okamžite	Okamžite
7		Okamžite	Okamžite	2 sekundy	7 sekúnd	31 sekúnd
8		Okamžite	Okamžite	2 minúty	7 minút	39 minút
9		Okamžite	10 sekúnd	1 hodina	7 hodín	2 dni
10		Okamžite	4 minúty	3 dni	3 týždne	5 mesiacov
11		Okamžite	2 hodiny	5 mesiacov	3 roky	34 rokov
12		2 sekundy	2 dni	24 rokov	200 rokov	3 tis. rokov
13		19 sekúnd	2 mesiace	1 tis. rokov	12 tis. rokov	202 tis. rokov
14		3 minúty	4 roky	64 tis. rokov	750 tis. rokov	16 mil. rokov
15		32 minút	100 rokov	3 mil. rokov	46 mil. rokov	1 mld. rokov
16		5 hodín	3 tis. rokov	173 mil. rokov	3 mld. rokov	92 mld. rokov
17		2 dni	69 tis. rokov	9 mld. rokov	179 mld. rokov	7 tln. rokov
18		3 týždne	2 mil. rokov	467 mld. rokov	11 tln. rokov	438 tln. rokov

Verejné WiFi siete

- Hrozba

- Free WiFi bez hesla = prostriedok pre odpočúvanie
- Verejné WiFi siete s pripojením sa pomocou QR kódu – presmerovanie na škodlivú webovú stránku
- Verejné WiFi siete na letiskách, v obchodných centrách a iných rozľahlých priestoroch – možnosť podhodenia falošnej WiFi siete



- Odporúčanie

- Ak je možné, overiť si „pravosť“ WiFi siete u prevádzkovateľa (zamestnanec reštaurácie, hotela...).
- Nepoužívať WiFi siete bez zabezpečenia šifrovaním.
- Ak nie je možné WiFi „overiť“, nevyužívať služby, kde je potreba prihlásenia sa (bankové platby, mail, prihlásenie sa do e-shopu a pod.).

Prenosné média

- Hrozba

- Strata média (USB, SD, CD, DVD), ohrozenie dôvernosti dát uložených na médiu
- Podhodenie média (najčastejšie USB kľúč) s nebezpečným obsahom
- Používanie súkromných prenosných médií zvyšuje riziko infekcie pri prenose medzi počítačmi
- Nebezpečenstvo „zdieľania“ médií

- Odporúčanie

- **Nevkladať nájdené USB kľúče do počítača**
- Šifrovanie obsahu na prenosných médiách
- Podľa možnosti nezdieľať USB kľúče
- Upraviť „AutoPlay“ nastavenie pre externé zariadenia



Fyzická bezpečnosť

- Hrozba

- Strata, krádež notebooku, mobilu
- Ponechanie zariadenia bez dozoru, neuzamknutá obrazovka
- Zle umiestnené pracovisko, možnosť odpozorovania prístupových údajov
- Prístupové údaje na odkazových lístkoch

- Odporúčanie

- Šifrovanie dát na zariadeniach
- Uzamykanie miestností, odkladanie papierových dokumentov, uzamykanie počítačov, politika hesiel
- Sprevádzanie cudzích osôb, dozor pri práci v zabezpečenom priestore

Výkon mobilných zariadení

MOBILE SECURITY

Predstavená 1.9.2000

> NOKIA3310 VS RAKETOPLÁN na Mesiac



TEAM Apollo 11



Apollo Guidance Computer



**1300 x slabší procesor
ako Nokia 3310**

Apple iPhone 12 dokáže vykonať približne 11 teraflopov alebo 11 biliónov operácií za sekundu.

Bezpečnosť mobilných zariadení

- Hrozba

- Mobil je „malým počítačom“, prístup k firemným dátam (maily, kontakty, dokumenty), ale nie je rovnako chránený ako počítač.
- Zneužitie mobilného zariadenia môže viesť k prieniku do firemnej siete.
- Falošné nabíjacie káble na verejných miestach

- Odporúčanie

- Pravidelné záplaty aj pre všetky inštalované aplikácie, antivírové riešenie
- Aplikácie len z oficiálnych zdrojov a redukcia požiadaviek aplikácie (napr. zdieľanie polohy)
- Viacnásobná autentifikácia pre prihlásenie sa
- Nezobrazovať hlásenia bez prihlásenia sa
- Nepoužívať cudzie (neoverené) nabíjačky

<https://shop.hak5.org/products/omg-cable>

Bezpečnosť domáceho prostredia - príklad



Volania ▾ Internet, TV a paušál ▾ Telefóny a zariadenia ▾ Služby ▾ Pomoc a podpora

TP-LINK TD-W8901GB



Volania ▾ Internet, TV a paušál ▾ Telefóny a zariadenia ▾ Služby ▾ Pomoc a podpora

Hľadám pomoc pre D-Link DIR-300

Internet ▾

TP-LINK

ostatné informácie

Ostatné informácie

Po správnom zapojení modem-routra a pripojení 192.168.1.1

Zobrazí sa výzva na zadanie:

Prihlasovacie meno: admin Heslo: admin

Po načítaní web rozhrania zariadenia v internetovom
Quick start – Run wizard

Hľadám pomoc pre:

Internet ▾

D-LINK ▾

D-Link DIR-300 ▾

hľadať

ostatné informácie

Ostatné informácie

UPGRADE FW PRE HW VERZIU B1 (D-LINK DIR-300)

Aktualizácia firmvéru môže vyriešiť problémy, ktoré môže mať predchádzajúca verzia firmvéru a zlepšiť jeho aktuálnu výkonnosť.

Postup pre upgrade FW:

1. Prihlase sa do GUI zariadenia cez internetový prehliadač: 192.168.0.1 (Prednastavené prihlasovacie meno: admin - heslo: prazdne)
2. Maintenance – Firmware Update – Firmware upgrade – Browse: lokalizujte na disku PC súbor s aktualizovaným FW dir300b_v2.06_f41a.bin
3. Upload

Home office – ideálny cieľ

- Hrozba
 - Nedostatočná bezpečnostná konfigurácia domáceho pripojenia (WiFi, „firewall“)
 - Prístup z domáceho počítača, ktorý má iné zabezpečenie
 - Ukladanie klasifikovaných dát/dokumentov na domácom počítači
 - Zdieľanie domáceho počítača s inými členmi rodiny – deti
- Odporúčanie
 - Základné bezpečnostné opatrenia na domácom firewalle
<https://www.incident.sk/riesenia-10-tipov-bezpecne-nastavenie-wifi-router/>
 - Konzultácia bezpečnostných opatrení s IT oddelením pre použitie vlastného počítača na firemné účely (patche, aplikácie, antivírová ochrana)
 - Ukladanie klasifikovaných dát do šifrovaného priestoru
 - Pri zdieľaní počítača pristupovať každý člen cez vlastný účet, účty nezdieľať

Záverečné odporúčanie

- Počet útokov radikálne rastie a dnes už NEEXISTUJE nezaujímavý subjekt.
- Kybernetická bezpečnosť sa neobmedzuje na „pracovisko“.
- Rozmýšľať, neklikať, neveriť ľacným a „zadarmo“ veciam
- Nenechať sa vystrašiť, vystresovať „akútnosťou“ mailu, telefonátu, SMSky
- Vzdelávať sa, čítať – to jediné, čo nám ešte dnes nedokážu ukradnúť, sú vedomosti (zatiaľ). Či? Neuralink.

Či ? Elon Musk – Neuralink.com

Elon Musk informuje o implantovaní čipu do mozgu človeka. Zdroj – Elon Musk/X



No questions please, I'm tired!

matej.peter@emsec.sk
podcast@incident.sk



!INC!DENT