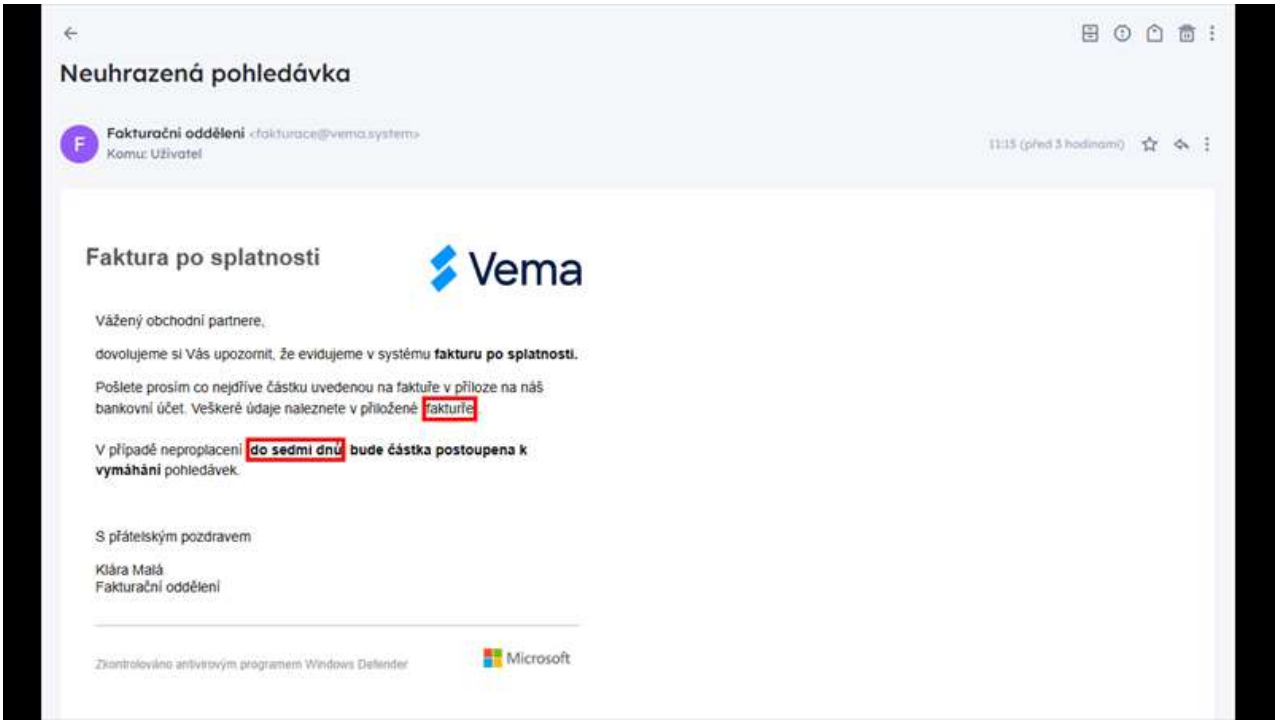
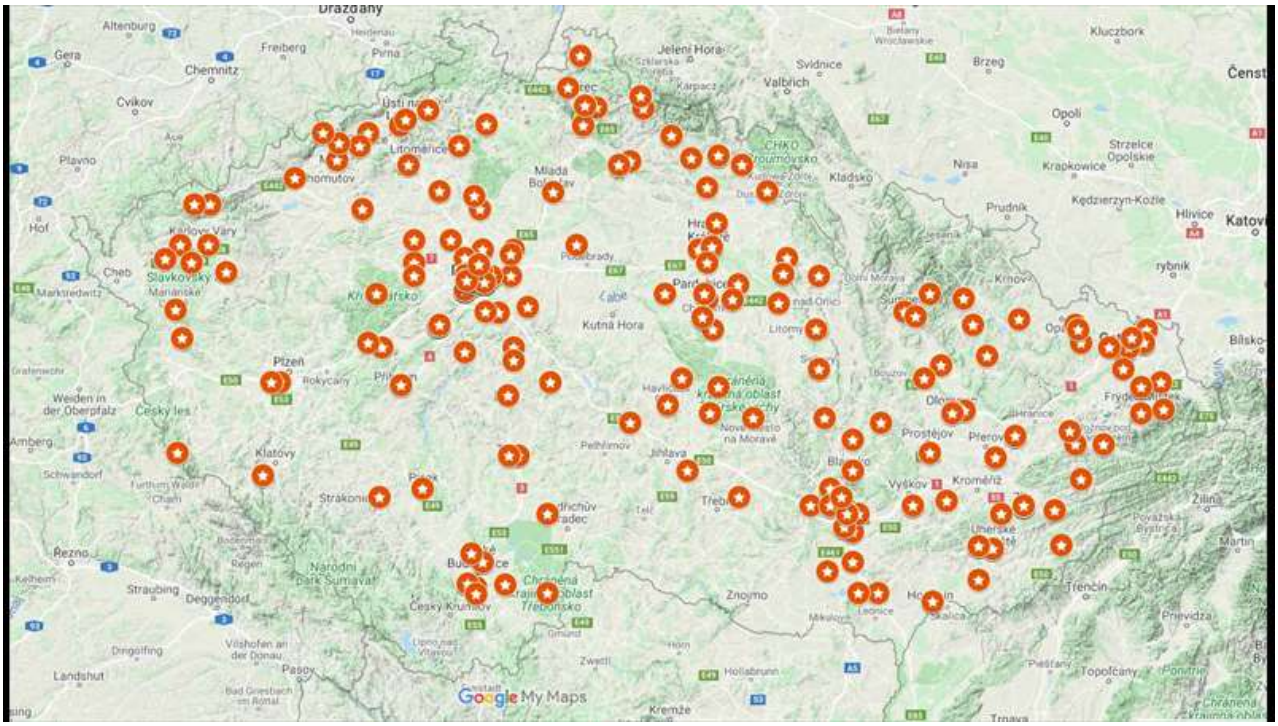
Etický hacker otestoval desítky českých institucí a firem. Některé dopadly naprosto tragicky

zive.cz/clanky/eticky-hacker-otestoval-desitky-ceskych-instituci-a-firem-nektere-dopadly-naprosto-tragicky/sc-3-a-230357/default.aspx

Jakub Čížek

24. září 2024




Google My Maps

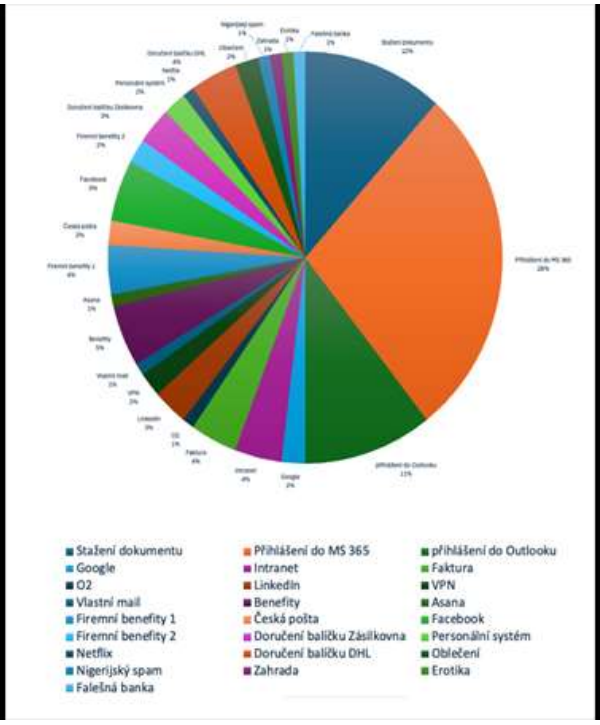

MIRKA_REDITELKA
PC-JIDELNA

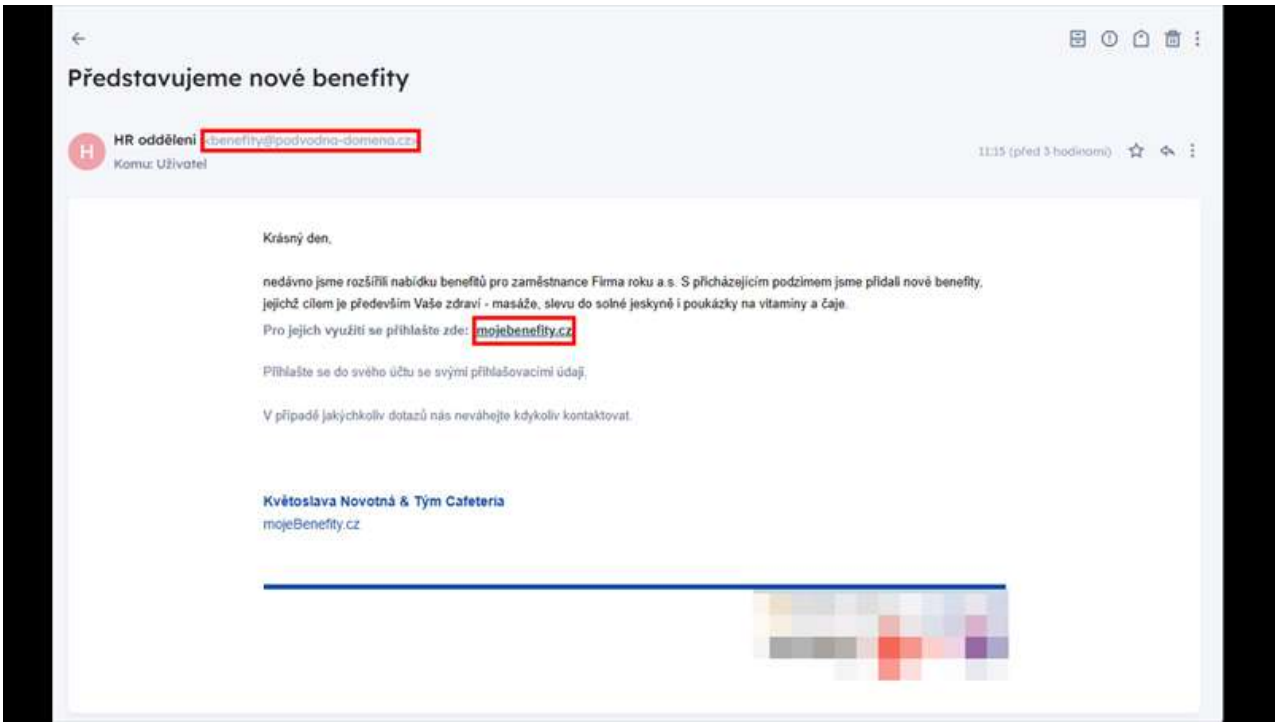
#phishing

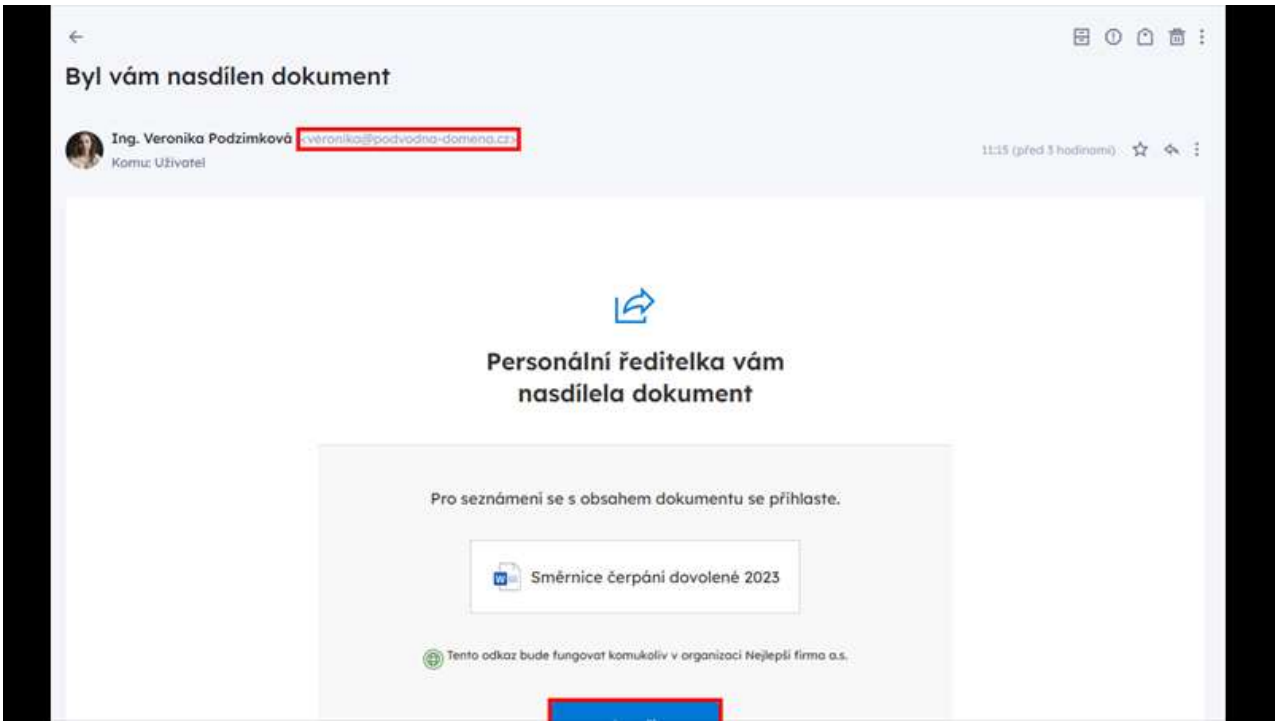
→ rozeslali jsme celkem 18 135 podvodných mailů

→ testovali jsme firmy a instituce napříč sektory:

- 6 nemocnic
- 39 soukromých firem
- 12 státních institucí
- 3 školy

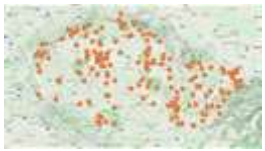






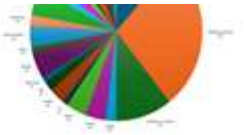
8

Fotogalerie



- Před pěti lety útočil Emotet. Podlehly mu nemocnice a OKD
- Soukromý i státní sektor od té doby masivně testuje zaměstnance
- Hackeři z BOIT Cyber Security rozeslali osmnáct tisíc e-mailů

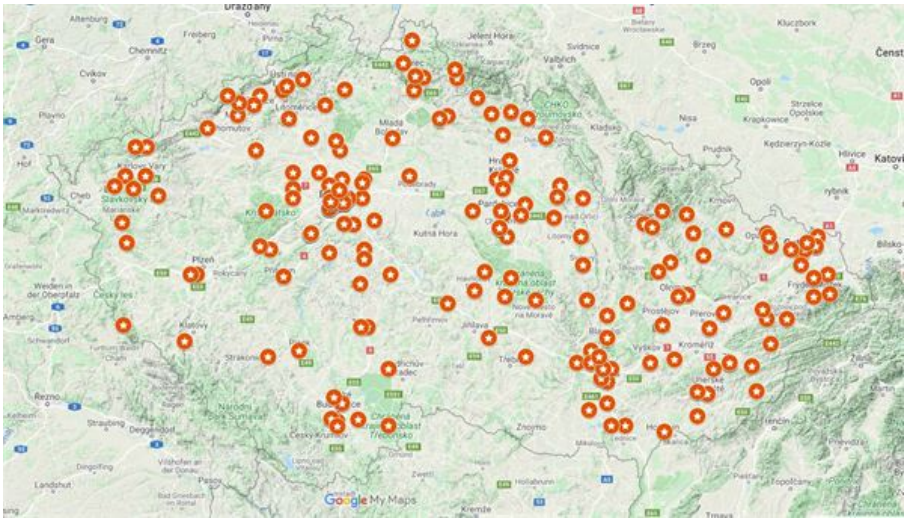
Když se mi před lety dostal do rukou seznam českých počítačů, na které tehdy útočil malware Emotet, bylo hned na první pohled jasné, jakým způsobem se dostal do vnitřní sítě obecních úřadů, škol i velkých firem.



Jen připomenu, že Emotet v roce 2019 úřadoval třeba v těžební společnosti OKD a na dlouhé hodiny prakticky vypnul i některé nemocnice.

Malware řádí v kancelářích

Když jsem se začetl do rozsáhlého seznamu IP adres, geografických lokací a síťových názvů počítačů, vyskakovala na mě jména jako **PC-UCETNI**, **UCETNIPC**, **KANCELAR**, **UCTO**, **BACK-OFFICE** a ano, byly tam i mašiny **REDITEL** a **REDITELKA**.



Některé zasažené počítače malwarem Emotet poté, co jsem je vynesl na mapu. Na seznamu bylo jak OKD, tak nemocnice, obecní úřady, vysoké školy...

Emotet se do sítě dostal skrze kanceláře bílých límečků, které velmi často klepli na to, na co neměli – typicky na zavirovanou přílohu v e-mailu, odkaz, který je dovedl na podvodnou stránku a tak podobně.

Sice měli ajťáky, ale také normální lidi

Emotet a další kauzy té doby jasně ukázaly, že i když můžete mít sebelépe zabezpečenou síť, nejslabším článkem je vždycky člověk, který s trochou štěstí leckde vyplní vlastní přihlašovací údaje,

protože ten formulář přece vypadal tak věrohodně a měl i logo naší firmy!

Není tedy divu, že někdy tou dobou začal soukromý i státní sektor masivně investovat do testování svých vlastních zaměstnanců a najatí etičtí hackeři měřili, kolik z nich kleplo na falešný e-mail.

Osmnáct tisíc e-mailů

Jedním z těchto etických hackerů je i Pavel Matějíček z BOIT Cyber Security, který se na nedávné konferenci CyberCon 2024 v režii Národního úřadu pro kybernetickou a informační bezpečnost pochlubil, jak na tom dnes jsme.

Z přednášky Pavla Matějíčka na letošním CyberConu

BOIT Cyber Security v posledních dvou letech otestoval více než **šedesát českých firem a institucí**, rozeslal dobrých **osmnáct tisíc falešných e-mailů** a mezi příjemci figurovaly jak nemocnice, tak školy, dvanáct státních institucí a čtyřicítka soukromých podniků.

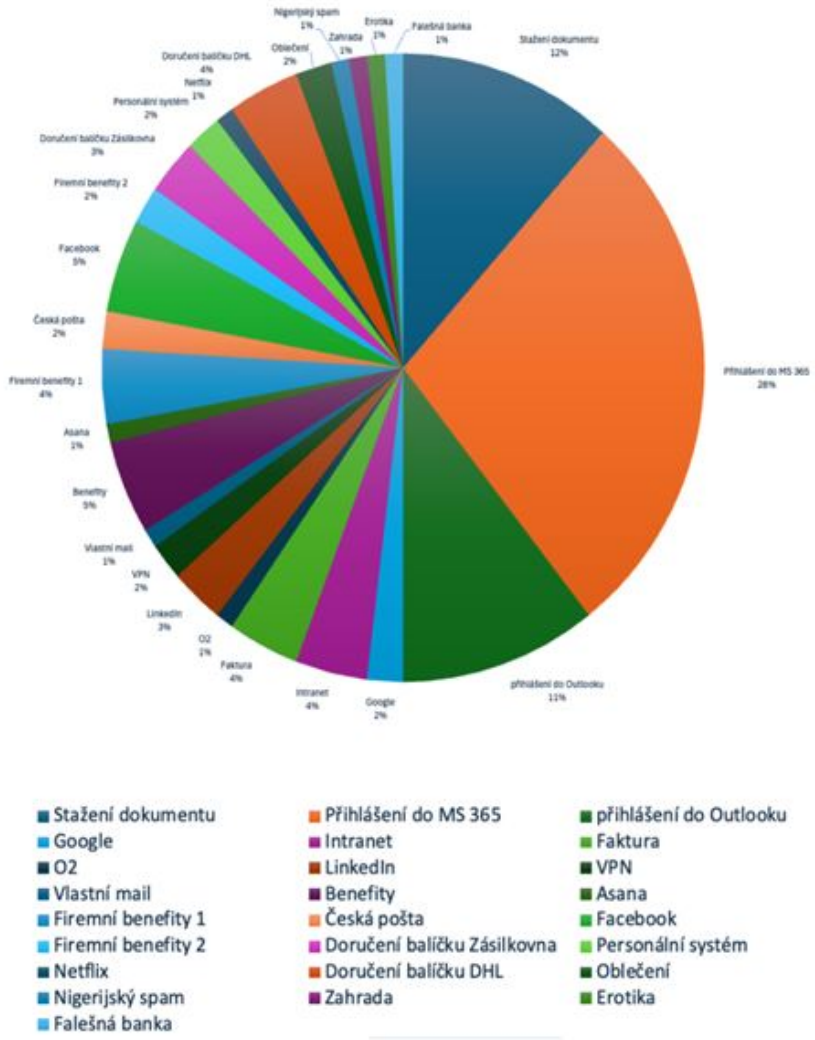
Jména si Pavel samozřejmě nechal pro sebe, na seznamu byste ale našli i známé značky, jejichž produkty dost možná používáte každý den.

Sestřičky nečtou e-maily

Tak a teď to nejhorší. Přes veškerou vzdělávací snahu v podnicích a v podstatě nepřetržitou medializaci stále klepáme tam, kam nemáme. Z celkového počtu **18 135 odeslaných**

phishingovych e-mailů totiž otevřelo simulovanou podvodnou stránku v průměru **26 % uživatelů**.

Nejohroženější skupinou byly školy, kde průměrná úspěšnost phishingu dosáhla dokonce 30 %. V případě státních institucí to dělalo 21 % a v soukromém sektoru 17 %.



Na co se zaměřují simulace phishingových útoků

Zajímavým případem jsou nemocnice s pouhými 7 % obětí, Matějíček ale vše uvádí na pravou míru: „Je to do značné míry způsobeno tím, že **v nemocnicích uživatelé maily často nečtou**, poměr těch otevřených je tedy nižší než jinde.“

Selhal skoro celý okresní úřad

Stále se však jedná o zprůměrované hodnoty. Kdybychom totiž chtěli vypíchnout některé krajní premianty, čísla jsou bez nadsázky katastrofální.

„Nejhorší výsledek jsme zaznamenali na jistém úřadu v nejmenovaném okresním městě, kde jsme **získali přihlašovací údaje od 59 % zaměstnanců**," přiznává Matějíček. Nejhorší testovaná soukromá firma pak dosáhla nelichotivého skóre 47 %.

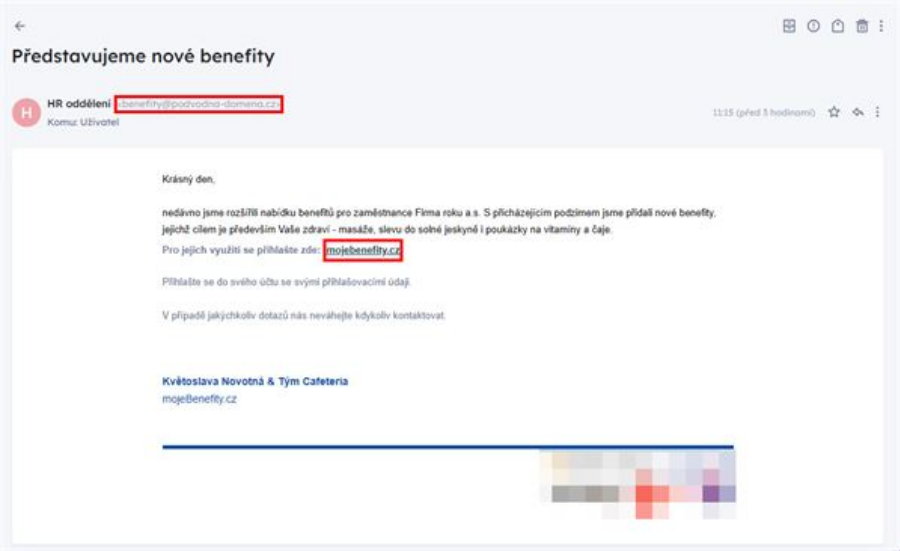
Éra „drahouška zákazníka" je ta tam

Čísla to jsou sice hrozivá, ale není se čemu divit, Matějíčkova firma totiž klientům pochopitelně neposílá dnes už legrační e-maily z dob kybernetického uhlí a páry. Zapomeňte na „drahouška zákazníka" z legendární kampaně, která před šestnácti lety útočila na klienty České spořitelny – teď žijeme v éře spear phishingu.

To znamená, že namísto natvrdlých textů si dávají autoři záležet a připraví záškodnický e-mail, který vypadá na první pohled opravdu věrohodně a často pracuje s vnitrofiremními informacemi. Stručně řečeno se jedná o pokročilý sociální hacking a často se napálí i ti, kteří přece nejsou žádná paka, a dokonce umějí doma nainstalovat i Linux!

Nabídněte nové benefity a úspěch je zaručený

Podle Matějíčka skvěle fungují zejména ty e-maily, které zaměstnancům slibují nějaký ten dáreček. Takže stačí, aby vám v poště přistála zpráva od fiktivního personálního oddělení, že se v novém roce navýší hodnota stravenek, a celý korporát s trochou nadsázky okamžitě klepne na (falešnou) verzi webu mojebenefity.cz.



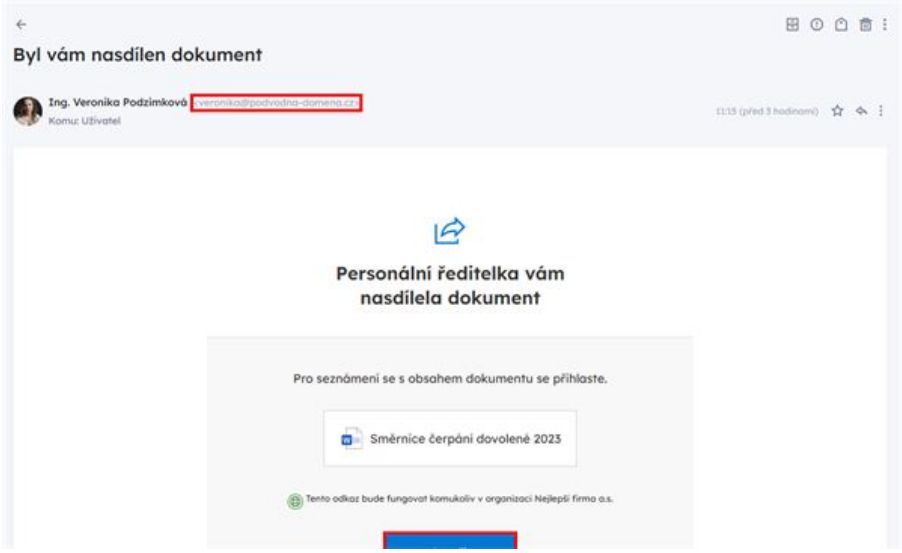
Stačí slíbit nový podnikový dárek a začnou na to klikat i ajťáci

„A přestože se později dozvědí, že to byla jen simulace a žádný bonus navíc z toho nebude, stejně ho požadují po vedení," pobaveně doplnil Matějíček, když jsem si s ním krátce popovídal u nás v redakci.

Školy by na tom měly být nejlépe, ale je to průšvih

Úřady a firmy nicméně ať vezme čert – horší je to s těmi školami. Kde jinde by to mělo fungovat než právě tam, kde se příští generace připravují na reálný život, který se dnes velkou měrou odehrává právě online.

V tomto směru představuje 30% průměrná úspěšnost phishingových simulací naprostou katastrofu. A pokud si teď řeknete, že holt starší pedagogové občas selžou, protože internetu nerozumějí, testování dětí, kterým se BOIT Cyber Security také věnoval, nedopadlo o moc lépe.



Pozor, dorazil e-mail, který se týká dovolené. I toto zaujme skoro každého

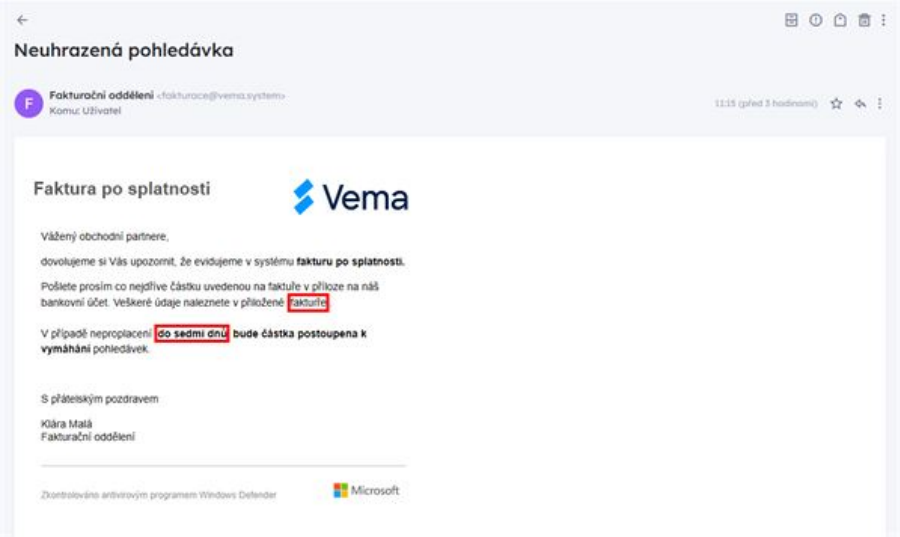
Zapomeňte na falešnou představu, že generace, která vyrostla na internetu, internetu také rozumí. Mnohdy platí pravý opak, z počítačů a všeho okolo se totiž už dávno stala spotřební elektronika, kterou prostě jen používáme a nevíme, jak opravdu funguje.

Počítače už nestavíme, ale kupujeme a stejně tak moderní automobil odvezeme do servisu a nebastlíme doma v garáži, protože je to prostě na rozdíl od staré škodovky po dědovi extrémně komplikovaný a čipy prošpikovaný stroj.

Je to už klišé, ale obranou je kybergramotnost

Podle Matějíčka by dnes proto mělo být minimální dobrou praxí alespoň zabezpečení každé organizace pomocí dvoufaktorové autentizace. Ta ledacos zachrání, i když dojde k podobnému úniku třeba formou phishingu.

„Nicméně ani 2FA neochrání firmy a instituce stoprocentně – klasické metody je totiž možné obejít za použití moderních technik," upozorňuje Matějíček.



Pozor, nová faktura. Rychle na ni klepnu, protože jsem účetní

Jedinou obranou je tedy opět to, čím jsem tento článek vykopl – vzdělávání zaměstnanců, učitelů, dětí a úředníků, kteří jediní jsou nakonec pěšáky pomyslné kybernetické války.

Jen díky lepší kybernetické gramotnosti ubude oněch zasažených počítačů s názvy jako UCETNIPC, UCTO a REDITEL. **V roce 2024 je už vážně pozdě na výmluvy typu: „Ale já nejsem ajťák a těm počítačům vůbec nerozumím.“** Ostatně, na dálnici vás také nikdo nepustí, pokud neumíte řídit.