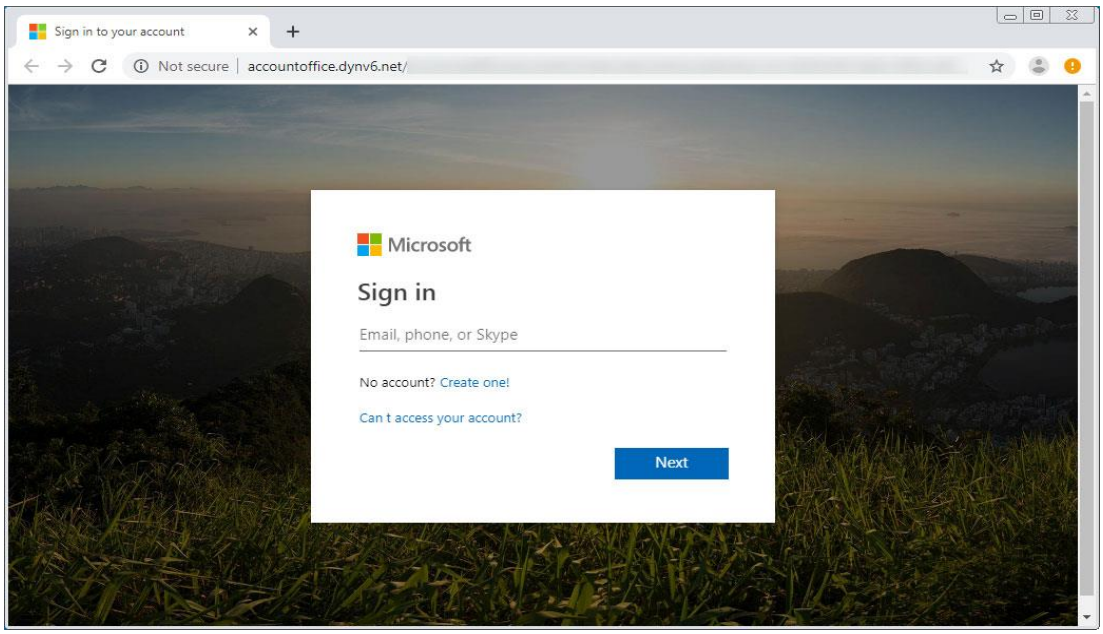
Zvýšená hrozba kybernetického útoku

V souvislosti se současnou situací na Ukrajině upozorňujeme na zvýšenou hrozbu **kybernetických útoků**, zejména ve formě **phishingu**.

Phishing je forma útoku **založená na sociálním inženýrství**, zpravidla se útočníci pokoušejí získat přihlašovací údaje, důvěrné informace nebo doručit do vašeho počítače nebo celé sítě škodlivý software prostřednictvím emailu. Jednoduše řečeno, kyberútočníci se chtějí prostřednictvím phishingového emailu **vlámat do vaší instituce.**

!!! Neotvírejte, nestahujte přílohy a neklikejte na odkazy podezřelého emailu.
V případě pochybností se prosím obraťte na administrátora (správce sítě) !!!

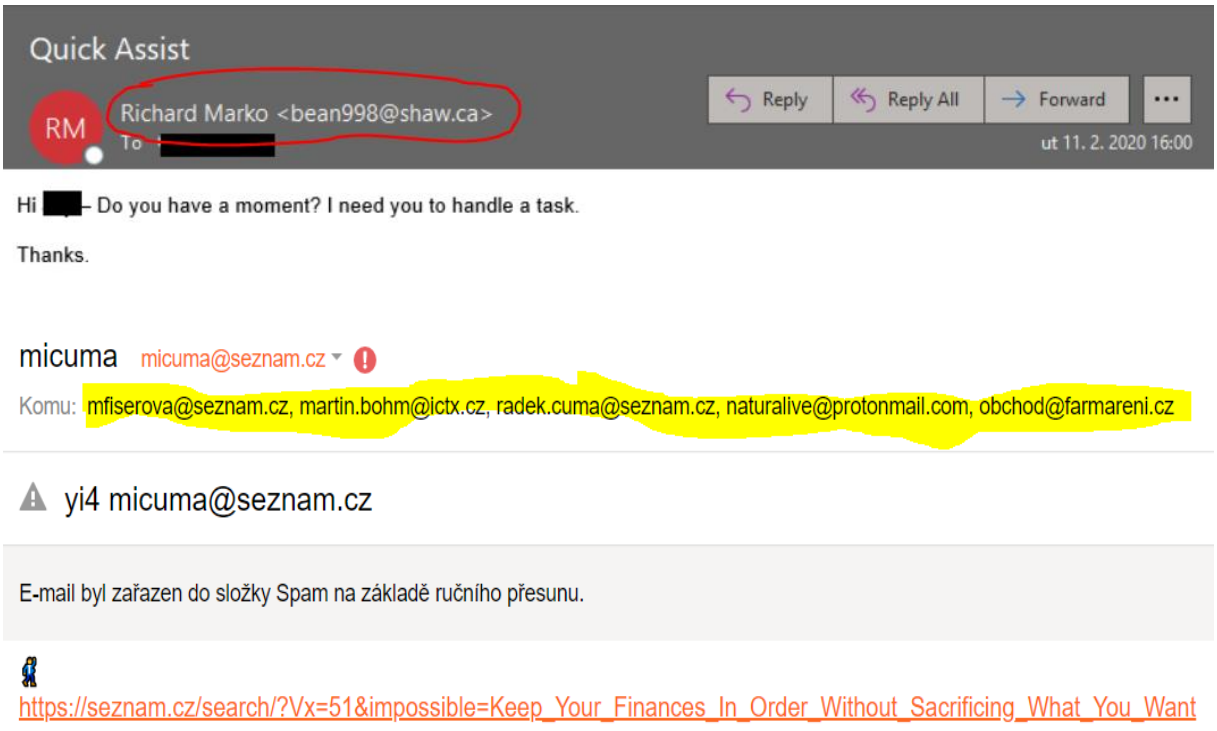


Phishingová stránka, které sbírá přihlašovací údaje do služby Office 365

Jak poznat phishingové a škodlivé emaily

1. E-mailová adresa

Neshoda jména a emailové adresy, podezřelá emailová adresa, eventuálně podezřelé emailové adresy dalších příjemců



2. Pozdrav a úvod e-mailu

Pozdrav může napovědět, zda je odesílatel důvěryhodný. Na oslovení „Milý zákazníku/Vážená paní, Vážený pane“ není co zkazit, na druhou stranu vypovídá o tom, že odesílatel vlastně o vás a vaší firmě nic neví.

3. Přílohy a odkazy jsou nejhorší !!!!!!!!!!

Phishing stojí za 32 % bezpečnostních incidentů. Pokud se vám odkaz či příloha nezdá, neklikejte na ně. Pokud myší najedete na text odkazu, zobrazí se vám cílová URL adresa. V případě podezření se poraďte s vašimi IT specialisty.

4. Špatná gramatyka (názorná ukázka)

Nekvalitní text je častý znak phishingu. Pokud uvidíte neobvyklá slova, strojový překlad, chybně napsaná slova, nereagujte na nic v e-mailu. Útočníci často používají překladače, naštěstí v případě češtiny jsou značně nedokonalé.

5. Urgentní požadavek

Útočníci chtějí, aby adresát zpanikařil a zareagoval hned, než si stihne uvědomit, že jde o podvod. Jakmile obdržíte e-mail, který po vás vyžaduje okamžitou aktualizaci hesla, rychlé provedení platby nebo jinak útočí na emoce, mějte se na pozoru. Případně si ověřte požadavek nezávisle na e-mailu. Nevěřte tlaku vyvíjeném v e-mailu. Častým argumentem je exekuce nebo zablokování nějakého účtu, tak to ale nefunguje. Žádná důvěryhodná společnost nevyžaduje reakci v řádu hodin.

6. Příliš dobré nebo děsivé zprávy

E-maily, které vám slibují pohádkové dědictví, výhru nového vozu nebo naopak vyhrožují ztrátou účtu na Instagramu jsou zpravidla podvod. Útočníci také často zneužívají populární služby, například obchody a dopravce. Ve druhém čtvrtletí tohoto roku byla nejzneužívanější značkou DHL. Pokud obdržíte zprávu, že není možné doručit zásilku, ačkoli žádnou nečekáte, mějte se na pozoru. Případně se ke službě přihlaste přes oficiální stránky, nikoli tlačítko v e-mailu.

7. Neobvyklé načasování

Phishingové e-maily často dorazí do schránek v nočních hodinách. To proto, že útočníci pracují v jiném časovém pásmu. Pokud obdržíte mail od kolegy, že potřebuje proplatit fakturu v 3:24 ráno, jsou možné jen dvě varianty: kolega je workoholik nebo jde o podfuk

8. Předmět a obsah nesouhlasí

Předmět slouží jako shrnutí konverzace. Pokud se v předmětu mluví o jablkách a v těle e-mailu o hruškách, je něco špatně.

Zdroj informací

ESET internet security: Phishing stojí za třetinou průniků: Jak poznat škodlivé e-maily? Dostupné z: https://www.eset.com/cz/blog/prevence/phishing-stoji-za-tretinou-pruniku-jak-poznat-skodlive-e-maily/