Trénujeme ostražitost na internetu

22.10.2025 - Radek Pirkl | Technická univerzita v Liberci

Naši ajťáci spustili testovací phishingovou kampaň zacílenou na studující i zaměstnankyně a zaměstnance. Výsledek? Je rozhodně na čem pracovat.

„Podvodné emaily vyzývaly pod různou záminkou k zadání přihlašovacích údajů do centrálního systému TULky, do sítě LIANE. Rozeslali jsme skoro 11 500 mailů, které se z uživatelek a uživatelů snažily vylákat citlivé údaje, a celkem se nám v tom dařilo, i když podvodné maily nepatřily k těm nejsofistikovanějším,“ říká vedoucí Oddělení informačních systémů TUL Jan Rous. Maily posílali od dubna do června 2025.

Podle prorektora TUL pro informatiku Pavla Satrapy odpovědělo na mail zadáním platných přihlašovacích údajů více jak 12 % uživatelek a uživatelů.

„Dalších 10 % oslovených na phishingový mail reagovalo nebo zadalo neplatné údaje. Nemáme srovnání po fakultách, ale můžeme ještě dodat, že u studujících nám vyšlo číslo úspěšně napálených dokonce o něco vyšší – 16 %,“ říká Pavel Satrapa s tím, že na studentky a studenty cílila koncem června masivní kampaň a počet oslovených je tak vyšší.

František Tomeš, manažer kyberbezpečnosti TUL, přidává srovnání, že u podobně velkých univerzit nebo korporátů bývá „úspěšnost“ phishingových kampaní zhruba pětiprocentní. Tyto instituce se však podle Tomeše k výrazně nižším číslům dopracovaly školeními a tréninkem. Máme tedy na TULce na čem pracovat.

„Při správě vlastní pošty je potřeba být stejně obezřetný, jako jste, než třeba pustíte někoho k sobě do bytu. S phishingovým mailem bude něco v nepořádku: už podoba adresy odesílatele, oslovení, stylizace vět, pokyn nebo žádost, kterou nám odesílatel zadává. Těch atributů je celá řada. Je dobré naučit se to rozlišovat, protože s nástupem AI bude phishing stále více propracovanější,“ říká František Tomeš a dodává: *„Nejlepší je takovou poštu neotvírat a hned házet do koše. Když si nejste jistí, na mail určitě neodpovídejte a adresátovi, který se tváří, že je to někdo z kolegů nebo z Vašeho okolí, raději zavolejte.“*

„V podobném testování budeme určitě pokračovat. Ukázalo se, že má smysl. Naším cílem je zvýšit povědomí lidí na TULce o kyberbezpečnosti, a tím předejít kyberútoku, který by po phishingové kampani mohl následovat. Ke zvýšení odolnosti našich uživatelů přispívá i online kurz kybernetické bezpečnosti, který jsme vytvořili v české i anglické verzi,“ dodává prorektor Satrapa.

Kurz kyberbezpečnosti TUL

Kurz jsme spustili k prvnímu září, je určený především zaměstnankyním a zaměstnancům TULky. Už po měsíci provozu se jich na kurz přihlásila zhruba polovina. Kurzy vytvářeli manažer kyberbezpečnosti spolu s lidmi z oddělení informačních systémů.

„Vycházeli jsme z platné legislativy a inspirovali se i kurzy, které na trhu už jsou. Kurz je určený všem, kteří na TUL pracují, tedy od technických pracovníků přes administrativní aparát až po akademiky. Součástí je i závěrečný test. Obtížnost jsme zatím volili velmi mírnou,“ říká František Tomeš a dodává, že výhledově přibyde také kurz kyberbezpečnosti pro vedoucí pracovníky nebo studující.

Jak prokázala phisingová kampaň, osvěta i mezi studujícími má rozhodně smysl. Generace Z se sice s

naprostou samozřejmostí pohybuje a orientuje v online prostředí prostřednictvím chytrého telefonu, ale neznamená to, že je ostražitější.

Zaměstnanci i studující, kteří během phishingové kampaně reagovali na podvodný mail zasláním platných osobních údajů, následně obdrželi mail s vysvětlením a také s výzvou, aby si změnili svá přístupová hesla.

„Lze totiž předpokládat, že se někdy v minulosti už nechali při phishingu vedeném zvenčí nachytat a své údaje zaslali,“ uzavírá Jan Rous.

Radek Pirkl

https://tuni.tul.cz/a/trenujeme-ostrazitost-na-internetu-164488.html