Češi a kybernetické hrozby. Co říkají výsledky průzkumu Zlaté koruny

17.7.2024 - | PROTEXT

Internet je plný úžasných možností, ale skrývá i nebezpečí. Kybernetické útoky se stávají stále častějšími a důmyslnějšími, a proto je důležité být obezřetní a chránit se. „Z výzkumu vyplývá, že necelé třetině populace se stala nějaká podoba kybernetického útoku. Více než pětina z nich přišla o finanční prostředky," uvádí Michal Straka, Product & Business Development Director Ipsos.

Důvěra v banky

Výsledky průzkumu ukazují, že Češi věří, že banky ochrání jejich finance. Celkem 89 % respondentů důvěřuje bankám, z toho 38 % velmi a 51 % spíše důvěřuje. Zajímavé je, že mladí lidé ve věku 25-34 let mají největší důvěru (95 %), stejně tak obyvatelé větších měst s více než 100.00 obyvateli (94 %) a Pražané (97 %).

Kybernetické útoky

Třetina respondentů (31 %) se setkala s nějakou formou kybernetického útoku. Nejčastěji šlo o phishing (47 %), malware (26 %) a krádež identity (31 %). Alarmující je, že více než pětina (21 %) těchto obětí přišla při útoku o finanční prostředky.

Informovanost o kybernetických rizicích

Informace o kybernetických rizicích získávají lidé nejčastěji z médií (42 %), sociálních sítí (27 %) a od bank (27 %). Přestože 82 % respondentů si myslí, že banky informují o těchto rizicích dostatečně, stále je prostor pro zlepšení.

Sebehodnocení a ochranná opatření

Více než polovina respondentů (57 %) se hodnotí jako osoby se středními znalostmi v oblasti kybernetických rizik, zatímco 5 % se považuje za experty. Z těch, kteří se považují za experty, používá 78 % dvoufázové ověřování a 72 % silná hesla, což je více než u obecné populace (62 % a 58 %).

Odpovědnost za kybernetické útoky

Průzkum také zkoumal názory na to, kdo by měl nést odpovědnost za újmu způsobenou kybernetickým útokem. Nejvíce respondentů (41 %) si myslí, že by to měla být finanční instituce, která byla cílem útoku. Dalších 29 % viní jednotlivce, pokud nedodržel bezpečnostní pokyny, a 26 % odpovědnost přisuzuje vládě a regulátorům.

Útoky přes email

Podle průzkumu 36 % respondentů někdy otevřelo podezřelý email, přičemž 44 % z nich nerozpoznalo, že jde o podezřelý email. Naopak 64 % respondentů podezřelý email neotevřelo, z nichž 51 % email bez otevření smazalo a 32 % ho přesunulo do spamu.

Role vlády

Pokud jde o vládní opatření v boji proti kybernetickým hrozbám ve finančním sektoru, respondenti by preferovali především vzdělávání a zvyšování povědomí o kybernetické bezpečnosti (33 %). Následuje tvorba a prosazování zákonů (22 %), spolupráce s bankami a dalšími finančními institucemi (22 %) a podpora výzkumu a vývoje (20 %).

Kompletní závěry z výzkumu můžete najít ZDE.

A jak se chovat v online prostředí, abyste minimalizovali riziko kybernetických útoků?

Ochrana bankovního účtu:

Ochrana před kybernetickými útoky:

V případě kybernetického útoku:

Kybernetická bezpečnost je důležitým tématem, které se týká nás všech. *„Průzkum Zlaté koruny ukázal, že Češi si uvědomují rizika spojená s kybernetickými útoky a aktivně se snaží chránit své finanční prostředky a osobní údaje. Důvěra v banky je vysoká, ale je potřeba pokračovat v informování a vzdělávání veřejnosti, aby byla schopna lépe čelit kybernetickým hrozbám“, říká Pavel Doležal, ředitel a zakladatel nezávislého vzdělávacího a informačního projektu Zlatá koruna a dodává: „Umělá inteligence, AI nám přináší zcela netušené příležitosti, ale bohužel také rizika. A jako zcela zásadní a neúčinnější obranu proti nim považuji prevenci, tedy informovanost a vzdělanost co nejširší populace“*. Klíčová pro zajištění kybernetické bezpečnosti v České republice bude také spolupráce mezi vládou, finančními institucemi a médii.

https://www.ceskenoviny.cz/tiskove/zpravy/cesi-a-kyberneticke-hrozby-co-rikaji-vysledky-pruzkumu-zlate-koruny/2544267