**7 tipů k bezpečnějšímu chování na internetu**

**Praha, 24. ledna 2023 -** Dodržovat základní pravidla bezpečného chování na internetu je vhodné pro každého, kdo se na něm pohybuje. Přinášíme několik tipů, které se vyplatí dodržovat, pokud chcete být na internetu v bezpečí.

**Hesla jsou základ. Musí být bezpečná, ne jednoduchá**

Mnoho lidí stále ještě vytváří velmi slabá hesla, a to kvůli snadnému zapamatování nebo také často nemění defaultní hesla pro přístup ke správě zařízení. Vedle toho, že nastavují hesla slabá je problém také to, že často volí u všech zařízení stejná.

„Uživatelům bych doporučil nastavovat si hesla silná a jedinečná pro každé zařízení. Tam, kde je to možné pak nastavit i jiné bezpečnější možnosti ověřování, například pomocí certifikátů. Uživatelé by také měli dbát na pravidelnou aktualizaci softwaru svých zařízení,“ říká Roman Kümmel, odborník na IT bezpečnost z Počítačové školy GOPAS.

**Na osobní údaje buďte opatrní**

Vždy si dobře rozmyslete, komu na internetu poskytnete své osobní údaje. Jméno, adresa, emailová adresa, soukromý telefon a jiné citlivé údaje jako je třeba rodné číslo. Velmi citlivé je také zadávání platebních údajů. Ty udávejte jen a pouze v rámci ověřeného internetového bankovnictví, případně v důvěryhodných platebních branách. Pokud byste měli platit z veřejných míst na veřejné Wi-Fi dávejte ještě větší pozor. Pokud to není bezpodmínečně nutné, vyčkejte na bezpečnější připojení.

**Zejména při placení dávejte pozor**

Stále častěji se objevuje trik podvodníků vydávajících se za pracovníky banky, kteří zjistili napadení bankovního účtu a snaží se oběť přesvědčit, že jediná cesta k ochraně je převedení financí na jiný účet. Útočníci k přesvědčování využívají nejčastěji telefonního hovoru.

„Podobných útoků celosvětově přibývá a zaznamenáváme i nárůst takových kampaní v českém jazyce. Často se také jedná o útoky cílené, kdy se útočník zaměří na svou oběť, zná její záliby, rutiny a dle toho vymýšlí taktiku útoku. Rozpoznat, že se jedná o útok, bývá často velmi náročné i pro IT profesionály. Z těchto důvodů je nutné myslet na zabezpečení počítačů, mobilních telefonů, ale i síťových prvků, které každodenně používáme,“ říká Michal Merta, ředitel pražského Cyber Fusion centra společnosti Accenture.

**Obezřetně na e-shopech i na e-bazarech**

Zneužití on-line prodejů je lákavý cíl. I když se může zdát, že podvodným e-shopům už lidé neuvěří, pořád jde o úspěšnou metodu podvodu. Protože stále více lidí nakupuje prostřednictvím mobilních telefonů, váží se k tomu i podvodné aplikace, navázané na konkrétní prodejce.

Naletět můžete i při koupi zboží přes e-bazary, kdy z kupujících chtějí podvodníci vylákat údaje o platebních kartách. Častou metodou je přesměrování na jakýsi oficiálně vypadající formulář, do kterého by kupující měl vyplnit údaje o své platební kartě – buď kvůli úhradě nebo dopravě zboží.

Lidé by nejen při nakupování, ale při jakékoli činnosti v kyberprostoru, měli zpozornět, pokud je po nich vyžadováno cokoliv nestandardního. Žádné citlivé údaje, jako jsou informace o platebních kartách, přístupových heslech do internetového bankovnictví nebo heslech do důležitých služeb, by neměli nikdy sdělovat dalším osobám, a to jak osobně, tak na vyžádání po telefonu či e-mailu.

**Stahujte jen ověřený obsah**

Pokud stahujete hry, soubory, fotografie, videa či další obsah, dělejte to vždy prostřednictvím důvěryhodné platformy. Mnoho internetových stránek totiž nabízí obsah neověřený. A takto můžete své zařízení, ať už se jedná o počítač, telefon nebo tablet, snadno nakazit malwarem, který má často podobu populárních her nebo užitečných aplikací. Dopady mohou být různé. Zařízení se může zpomalit, naruší se jeho fungování, nebo bude ukradena část či veškerá vaše data. Útočníkem získaná data mohou být následně ve velké míře zneužita.

**Používejte antivirové programy**

„Pro větší bezpečnost na internetu se vyplatí investovat do softwaru pro internetovou bezpečnost. Antivirové programy totiž dokáží odhalit většinu malwarových hrozeb a chránit tak v první řadě vaše soukromí a počítač. Spolu s opatrností a dodržováním dalších pravidel to výrazně pomůže zajistit vaši bezpečnost na internetu,“ radí Ondřej Ševeček, odborník na bezpečnost z počítačové školy GOPAS.

**Buďte opatrní při využívání veřejných počítačů**

Rizikem je i využívání veřejně přístupných počítačů – například na úřadech, v hotelu, kempu nebo v internetové kavárně. Při otevření prohlížeče z veřejně dostupného počítače využijte anonymních oken.

„Nezapomínejte po sobě zavřít použité aplikace a okna prohlížeče, odhlásit se z mailových profilů. Rozhodně nenechávejte uložená jakákoli přístupová hesla. Anonymizovaný prohlížeč po zavření okna smaže veškeré vámi vyhledávané informace a jiní uživatelé nebudou mít přístup k historii vámi navštívených stránek, dokonce ani k vašemu e-mailu. A pokud si sebou přinesete nějaká data na USB paměti, nezapomeňte ji v portu,“ říká Michal Černý, odborník na komunikační techniku ze společnosti Audiopro.