Microsoft u příležitosti mezinárodního Dne bezpečnějšího internetu, který tento rok připadl na 5. února, vytvořil bezplatnou vědomostní hru pro děti a příručku, jak uspořádat workshop a řídit diskusi. Společnost tak chce pomoct dospělým vést s dětmi debatu o bezpečnosti na internetu.

Firma zveřejnila také osm jednoduchých kroků, které lidem pomohou pracovat, ale i hrát hry, nakupovat a žít online co nejbezpečnějším způsobem.

1. SLOŽITÁ A ODLIŠNÁ HESLA

Pokud má někdo klíč od vašeho domu, může vstoupit a vloupat se do všech místností. Totéž platí pro hesla a online účty. Příliš často volíme hesla, která jsou snadno zapamatovatelná, jako jsou jména nebo data narození. Pokud je však pro vás snadné si heslo zapamatovat, je pravděpodobné, že se ho kyberzločincům také podaří snadno uhodnout. Používáte-li stejné jednoduché heslo pro více účtů, pak kyberzločinci mohou být (a také budou) schopni získat přístup ke všem vašim citlivým osobním údajům.

K bezpečnému ukládání více hesel pro různé účty používejte správce hesel. Vždy vytvářejte složitá hesla obsahující nejméně 10 znaků, které jsou kombinací číslic, malých a velkých písmen a speciálních znaků.

2. POZOR NA NEZNÁMÉ LIDI

Ne každý, s kým se seznámíte online, je tím, za koho se vydává. Je běžné, že kyberzločinci si na sociálních médiích vytvářejí falešné profily, aby navázali vztah s neopatrnými uživateli a poté odcizili jejich data nebo provedli ještě něco horšího.

Pokud vás osloví online neznámá osoba, která naléhá, abyste jí sdělili své osobní údaje nebo přímo požaduje peníze, měli byste se mít na pozoru. Pokud je to možné, zkuste tuto osobu přímo vyhledat, abyste zjistili, zda je příslušný účet věrohodný. Nejste si jistí identitou dotyčné osoby, ale přesto chcete přijmout její žádost o přátelství? V takovém případě ale pro jistotu omezte prostřednictvím nastavení ochrany osobních údajů informace, které si může daná osoba zobrazit o vašem profilu. Nezapomeňte: Pro online komunikaci platí stejná pravidla jako v reálném světě, a proto cizím osobám nesdělujte citlivé nebo soukromé informace.

3. OFFLINE NÁSLEDKY

Představte si internet jako náměstí nebo chodník. Je to veřejný prostor, ve kterém může každý spatřit nebo sdílet všechno, co publikujete. A to bez ohledu na to, zda je pro něj publikovaný obsah určený nebo zda jste mu dali svolení.

Než něco zveřejníte online, zvažte, zda chcete, aby se s tím mohl seznámit váš zaměstnavatel, zákazník nebo příbuzný. Dokonce i informace, jako je váš rodinný

stav nebo soukromá adresa, které se možná zdají neškodné, mohou být zneužity, pokud je získají nesprávné osoby.

4. CHRAŇTE SVÁ DATA

Až na několik výjimek bohužel neexistuje způsob, jak trvale odstranit obsah zveřejněný online. Všechny obrázky, komentáře nebo fotografie, které zveřejníte online, zůstanou pravděpodobně zveřejněné navždy. I když odeberete původní příspěvek, nebudete mít nikdy jistotu, že si jiní uživatelé nevytvořili kopie nebo že nesdílejí váš obsah v jiných sítích. Takže nevkládejte online nic, co nechcete, aby spatřily jiné osoby.

5. KLIKEJTE OPATRNĚ

Vyzkoušenou a v praxi ověřenou taktikou kyberzločinců je přimět vás lstí, abyste si stáhli malware, který jim umožní odcizit vám informace. Malware může být maskován různými způsoby – od oblíbené hry po email nabízející technickou podporu. Vyvarujte se stahování aplikací, které vypadají nezvykle nebo pocházejí z neznámého webu. Nejste si jistí, jestli je určitý e-mail legitimní? V takovém případě si položte následující otázky: Má odesílatel podivnou emailovou adresu? Je oslovení neosobní? Obsahuje text spoustu pravopisných chyb? Snaží se působit podivně naléhavým dojmem?

Pokud si stále nejste jistí, obraťte se na příslušnou značku nebo společnost prostřednictvím oficiálních kanálů, jako je její web nebo stránka sociálních médií. Vždycky je lepší všechno třikrát ověřit než se vystavit riziku ohrožení zabezpečení.

6. NASTAVTE SI SOUKROMÍ I ANTIVIR

Když neaktualizujete prostředky, které používáte na svou obranu, kybernetičtí zločinci nakonec přijdou na to, jak ji překonat. Nezapomeňte udržovat operační systém v nejaktuálnějším stavu prostřednictvím aktualizací a řádně kontrolujte nastavení ochrany osobních údajů v používaných aplikacích a prohlížeči.

7. JEN BEZPEČNÉ PŘIPOJENÍ

Když používáte veřejné připojení k internetu, například Wi-Fi v nákupním centru, nemáte žádnou přímou kontrolu nad jeho zabezpečením. Pokud se nemůžete připojit bezpečně, nebo nevíte jistě, jestli je vaše zařízení chráněné, nesdílejte citlivé informace. Je bezpečnější počkat, až budete doma a budete moci použít zabezpečenou síť Wi-Fi.

8. POŽÁDEJTE O POMOC

Nikdy nepodléhejte pocitu, že kliknutí na odkaz nebo publikování příspěvku nepočká. Není nic naléhavějšího než vaše bezpečnost online.