5 tip til forebyggelse af svindel for ældre

Hvordan kan folk, der ikke er vokset op med teknologi, beskytte sig mod nogle af de mest almindelige former for onlinesvindel?

Den konventionelle måde at tænke på er, at mange aldrende mennesker har tendens til en højere risiko for at blive bytte for svindlere end deres børn eller børnebørn. Uanset om ældres øgede udsathed for svindel er sand eller ej, bliver ældre mennesker bedraget for enorme summer via forskellige typer svindelnumre, herunder tyveri, bedrageri og udnyttelse via internettet. Desuden vil sådanne statistikker sandsynligvis kun repræsentere en brøkdel af de faktiske skader, da mange ofre er for flove til at stå frem og indrømme, at de er blevet snydt af svindlere.

Men hvad er det, som gør mange ældre sårbare over for onlinesvindel? Svindlere kan bl.a. udnytte deres tillidsfulde natur og i nogle tilfælde forværrede kognitive evner forårsaget af aldring. Det er overflødigt at sige, at svindlere kan udnytte det faktum, at de tilsigtede ofre ikke voksede op med teknologi og aldrig fik selv den mest basale undervisning i cybersikkerhed.

Vær skeptisk

Antag aldrig, at du kan have tillid til en fremmed person online. Faktisk er det bedste råd altid at overveje muligheden for, at den uventede meddelelse kan være et forsøg på svindel. Det indebærer også, at du skal være forsigtig, selvom meddelelsen kommer (eller synes at komme) fra en person, du kender, og dette gælder ligeledes for meddelelser, der leveres via e-mail, chat, onlinemeddelelser eller sociale medier. Hold øje med noget usædvanligt ved meddelelsen eller afsenderen. Det kan være en svindler, der er kommet ind på din vens onlinekonto og bruger den til at sprede ondsindet spam. Smid den ud, hvis du er i tvivl!

Lad være med at klikke

Et phishing-angreb, som er en af de mest gennemgribende former for onlinesvindel, begynder typisk med en uopfordret e-mail eller en meddelelse på de sociale medier, hvor svindleren udgiver sig for en betroet enhed og vha. social engineering-teknikker forsøger at overtale dig til at udlevere dine følsomme data såsom kreditkortoplysninger eller legitimationsoplysninger til logon. Mange svindlere har udviklet sig til langt mere end forkert stavede og rent tekstbaserede phishing-meddelelser, og de har opbygget komplette kopiwebsteder og Facebook-sider med fristende kampagner. Du bør aldrig automatisk antage, at materiale modtaget ud af det blå – uanset hvor officielt det ser ud – er autentisk. Derfor skal du aldrig klikke på links eller åbne vedhæftede filer i e-mails, selvom meddelelsen ser ud til at komme fra en kendt, pålidelig kilde.

Sig nej, hvis det er gratis

Svindlere kan også sende dig en e-mail for at lykønske dig for din "gevinst" i et lotteri eller en konkurrence, du slet ikke har tilmeldt dig eller deltaget i. Men for at få udleveret din "præmie", beder de dig alligevel om dine personlige oplysninger og/eller anmoder om en betaling på forhånd i en slags "forudbetalingsfidus". Typisk vil den officielle skrivelse forsøge at foregive en slags hastende karakter og bede dig om at reagere hurtigt eller risikere at gå glip af muligheden. Husk, at legitime lotterier aldrig kræver, at vindere skal betale gebyrer for at få udbetalt deres gevinster.

Send aldrig penge til fremmede

Tillid/romantik-bedrageri, hvor offeret er lokket til at sende penge eller personlige oplysninger til en falsk beundrer, var den anden dyreste type onlinesvindel, der ramte folk i alle aldre i 2018. Romantik-svindel har i årevis stået højt på listen over de mest almindelige former for svindel rettet mod ældre. Det virker naturligt, idet ensomhed er et af de hyppigste problemer, som ældre har.

Læg på

I teknisk support-svindel vil svindlerne ofte forsøge at overbevise dig om, at din computer er blevet ramt af malware, og at du skal give dem fjernadgang til din enhed, så de kan løse problemet. Selvfølgelig er påskuddet falsk, men den efterfølgende skade – tabet af personlige oplysninger og penge – er meget reel. Du skal aldrig give en fremmed fjernadgang til din computer, selvom vedkommende hævder at repræsentere en velrenommeret leverandør.

Bonustip

Det sidste tip er primært henvendt til de yngre – lad os holde dialogen med vores forældre og bedsteforældre åben og forklare dem de grundlæggende praksisser for cybersikkerhed på en måde, der er til at forholde sig til. Ud over at få en bedre forståelse af farerne ved onlineverdenen vil mange af dem føle sig mere engagerede og mindre ensomme, og det kan i sidste ende hjælpe dem med at blive mere sikre online.