Pressemeddelelse

19. marts 2018

Sociale medier er et slaraffenland for IT-kriminelle

Danskerne er storforbrugere af internettet, men med mere tid online havner flere også i armene på onlinesvindlere og bliver ofre for IT-relateret bedrageri. Alka guider til, hvordan du begår dig sikkert på nettet, og hvordan du er dækket, hvis dine personlige oplysninger bliver stjålet og misbrugt.

Facebook, netbank, e-mail og NemID. Hver dag bruger danskerne tjenester på nettet, der kræver personfølsomme oplysninger. Men i takt med at vores liv rykker mere og mere online, er økonomisk kriminalitet på nettet som bedrageri og svindel fulgt med.

Ifølge Det Kriminalpræventive Råd blev 150.000 mennesker udsat for typiske former for IT-kriminalitet i 2015, og tal fra Rigspolitiet viser, at anmeldelser om IT-relateret bedrageri er steget fra 4.623 i 2009 til 20.428 i 2016 – det svarer til en stigning på 350 procent.[1]

Men ved at bruge sund fornuft, og ved at stille større krav til vores egen sikkerhed og adfærd i den virtuelle verden, kan vi selv være med til at bremse de IT-kriminelle, mener Kommunikationsdirektør i Alka, Lise Agerley.

- Vi lever en stor del af vores liv online, men med flere klik følger også en større risiko for at blive snydt på nettet. De IT-kriminelle tager mere og mere avancerede metoder i brug, så vi er alle i farezonen for, at vores personlige oplysninger havner i armene på onlinesvindlere. Konsekvensen er, at de enten bruger dit kreditkort eller misbruger din identitet, fortæller hun.

- Selvom det er en meget ubehagelig oplevelse at få stjålet sin identitet eller blive bedraget økonomisk, er du heldigvis godt beskyttet, hvis dine personlige oplysninger bliver brugt til svindel online. Dit betalingsinstitut er ansvarlig for at dække det økonomiske tab, hvis dine betalingskortoplysninger bliver misbrugt, og igennem indboforsikringen er der ofte hjælp at hente, hvis din identitet bliver stjålet - bl.a. til at begrænse skadevirkningerne af den svindel, de IT-kriminelle har foretaget i dit navn, og afvise uretmæssige krav fra kreditorer.

Lise Agerley guider her til fire tricks, de IT-kriminelle bruger online for at franarre dig personlige oplysninger og afpresse dig på nettet.

Fire tricks du skal passe på online

Pharming og phishing

Pharming og phishing er begge metoder, hvor de IT-kriminelle udgiver sig for at være en anden afsender og herigennem lokker oplysninger ud af dig. Det kan f.eks. være ved at kapre et websteds domænenavn og omdirigere brugerne til deres egen hjemmeside, hvor de let kan snuppe fortrolige data som konto- og kortnummer. Det kan også være ved at sende e-mails eller sms'er, der ser ud til at komme fra f.eks. SKAT eller Nets, hvori de beder dig om at klikke ind på et link og indtaste personlige oplysninger.

- Vær altid skeptisk, hvis du får en e-mail eller sms fra et ukendt telefonnummer eller en ukendt e-mailadresse med et mistænkeligt domæne i linket. Hold også øje med grammatiske fejl. Det er som oftest en god indikator på svindel. Som tommelfingerregel vil institutioner som SKAT aldrig bede dig klikke ind på et ukrypteret link og udfylde oplysninger, men derimod

[1] Rigspolitiets rapport "Styrket indsats mod økonomisk it-kriminalitet": https://www.politi.dk/NR/rdonlyres/D8031319-3B8B-48A0-ADB0-398BB73182EA/0/Styrketindsatsmodoekonomiskitkriminalitet_15052017.pdf

sende via e-Boks eller bede dig logge ind på en sikker forbindelse på egen hjemmeside igennem NemID, fortæller Lise Agerley.

Skimming
Når IT-kriminelle stjæler dine personlige oplysninger og bruger dem til at lave et falsk betalingskort eller pas med rigtige oplysninger, som de herefter misbruger, kaldes det skimming.

- Vær opmærksom på hvem du udleverer dine kreditkortoplysninger til. Sørg også for ikke at dele billeder på sociale medier, hvor de internetkriminelle kan lure pas-, konto- eller CPR-nummer. Selvom det er fristende at dele billeder af det nyerhvervede eksamensbevis, kørekort eller visum til en rejse på Instagram eller Facebook, kan oplysningerne hurtigt havne i de forkerte hænder, fortæller Lise Agerley.

Hvis du opdager, at dine kreditkortoplysninger er blevet misbrugt, skal du straks kontakte din bank og sørge for, at dine kort bliver spærret, råder hun.

Hijacking af profiler på sociale medier
Dine profiler på sociale medier er et slaraffenland af personlige oplysninger for de IT-kriminelle. Det kaldes 'hijacking', hvis en IT-kriminel får fat i dit login til f.eks. Facebook og fra din profil skaffer sig adgang til dine personlige oplysninger, researcher på dine venner og sender dem private beskeder med spam eller inficerede links, der kan slippe en virus løs hos modtageren, hvis vedkommende klikker på det.

- Selvom det er lettest at huske og bruge ét login til alle dine konti på nettet, gør det også arbejdet med at lure det lettere for onlinesvindlerne. Benyt forskellige logins til alle profiler, og gør dem komplekse ved at bruge en kombination af store og små bogstaver samt tal. På Facebook har du også mulighed for at slå login-notifikationer til under sikkerhedsindstillinger. Du vil herefter blive underrettet via sms eller e-mail, hvis nogen prøver at logge ind på din konto fra en computer eller telefon, der ikke er blevet logget ind fra før, og login kan ikke gennemføres, før du har givet tilladelse, forklarer Lise Agerley.

Ransomware
Ransomware er en virus, som låser alle dine filer ved at kryptere dem. Hackerne bag ransomwareangrebet kræver ofte en løsesum for at give dig adgang til filerne igen.

- Virus som ransomware finder vej i ind i din computer via smuthuller, der f.eks. opstår, hvis dine programmer ikke er up-to-date. Sørg derfor for at holde dit styresystem og antivirusprogrammer opdateret, så det bliver sværere for hackerne at skaffe sig adgang. Og tag en backup af dine filer jævnligt– enten online i cloudløsninger som Dropbox eller på en ekstern harddisk, så du altid har en ekstra kopi og kan genskabe dem på en ny enhed i værste tilfælde, fortæller Lise Agerley.

Hun råder også til, at man straks melder angrebet til politiet frem for at betale løsesummen.

For yderligere information kontakt venligst:
Lise Agerley, Kommunikationsdirektør i Alka
Direkte: 43 58 59 11 / Mobil: 40 21 01 77
lag@alka.dk