STYRK IT-SIKKERHEDEN

Faktaark med tips og tricks

telenor erhverv

3 tips til at undgå phising

Phishing-angreb er beskeder, der er designet til at ligne, at de kommer fra en pålidelig afsender.

Forestil dig, at du åbner, hvad du troede var en sikker e-mail, en sikker vedhæftning eller et ægte billede. I det næste sekund bliver du udsat for malware eller kriminelle, der vil have dine persondata. Men der er forholdsregler, der beskytter dig og virksomhedens data.

Lær at genkende tegnene og rapportér phishing.

Hold øje med disse tegn

- Stressende eller følelsesladet sprogbrug
- Krav om at opgive personlige eller økonomiske oplysninger
- Usædvanlige vedhæftninger
- Usikre og forkortede URL'er
- E-mailadresser, der ikke stemmer overens med den påståede afsender
- Dårligt sprog og stavefejl (mindre almindeligt nu)

Vent og rapportér

Rapportér mistænkelige beskeder til IT-afdelingen. Hvis henvendelsen udgiver sig for at komme fra en virksomhed, du stoler på, bør du også kontakte virksomheden direkte for at rapportere beskeden. Kontaktoplysninger kan findes på deres hjemmeside.

Slet

Slet beskeden. Svar ikke, og klik ikke på vedhæftninger eller links. Undgå også "Afmeld", da det sandsynligvis er en del af phishing-angrebet. Slet hele beskeden.

Hvis en besked ser mistænkelig ud, er det sandsynligvis phishing.

Selvom der er en mulighed for, at den kan være ægte, bør du ikke klikke på nogen af linksene, åbne vedhæftningerne eller ringe til nogen af telefonnumrene. Find i stedet en anden måde at kontakte virksomheden eller personen på ved at tjekke deres hjemmeside. Ring til personen på et kendt nummer og få bekræftet, at de har sendt dig beskeden.

Installer opdateringer

De fleste af os, der får besked om at opdatere software, trykker ofte “mind mig om det senere”. Men du bør tænke dig om to gange, før du udsætter det!

At holde din software opdateret er det bedste, du kan gøre for at være sikker online. Den nemmeste løsning er at slå automatiske opdateringer til.

Slå automatiske opdateringer til

Tjek indstillingerne på din enhed, sandsynligvis under Software eller Sikkerhed. Du kan også søge efter "automatiske opdateringer".

Hold øje med notifikationer

Ikke alle opdateringer sker automatisk. Enheder som mobiler, tablets eller laptops vil ofte give besked, når vi skal installere opdateringer. Det er vigtigt, at du installerer ALLE opdateringer, især dem, der gælder browsere og antivirussoftware.

Installer opdateringer så snart du kan

Hvis du får besked om softwareopdateringer, og især kritiske opdateringer, bør du installere dem så hurtigt som muligt. Cyberkriminelle venter ikke, og det bør vi heller ikke.

Hvorfor er det så vigtigt at opdatere regelmæssigt?

Hvis cyberkriminelle får adgang til en enhed gennem en sikkerhedsbrist, vil de lede efter personlige oplysninger og følsomme data, de kan udnytte.

Softwareudbydere sender opdateringer ud, der retter sikkerhedshuller så hurtigt som muligt. Hvis vi ikke installerer opdateringerne, kan de ikke beskytte os!

Softwareopdateringer kan også:

Fikse fejl

Forbedre ydeevnen

Installere de nyeste funktioner

Multifaktor-godkendelse

Sådan aktiverer du multifaktorgodendelse

MFA fungerer som et ekstra lag beskyttelse for vores onlinekonti og apps. Sikkerhedsmekanismen kan være en kode, der sendes som en tekstbesked eller genereres i en app. Det kan også være fingeraftryk eller ansigtsgenkendelse. Ved at bruge MFA bekræfter vi vores identitet på en sikker måde, når vi logger ind på vores konti.

Følg disse trin for alle dine konti:

1. Gå til Indstillinger
Almindelige betegnelser er Kontoinstillinger, Indstillinger og Privatliv eller tilsvarende.

2. Find MFA og aktiver det
Det kan også kaldes to-faktor-godkendelse eller totrinsverifikation.

3. Bekræft
Vælg, hvilken ekstra sikkerhedsforanstaltning du vil bruge. Du kan fx vælge at indtaste en kode, du får sendt via SMS eller e-mail, eller bruge ansigtsgenkendelse.

Tillykke!
Efter opsætningen af MFA kan du blive bedt om at gennemføre sikkerhedstrinet for at bekræfte din identitet. Det tager kun et øjeblik, men det gør os meget mere sikre i kampen mod ondsindede hackere. Aktiver MFA på alle onlinekonti, der tilbyder det.

Multifaktorgodkendelse beskytter vores:


E-mails


Kundeinfo


Finansielle data


Digital infrastruktur


Driftsdata

Stærke adgangskoder

Svage adgangskoder er den mest almindelige svaghed, der gør konti sårbare over for digitale angreb fra kriminelle.

Tre enkle tips til sikre adgangskoder

At bruge stærke adgangskoder ved hjælp af en adgangskodetjeneste er den nemmeste måde, vi kan beskytte vores konti og holde vores oplysninger sikre.

Lad adgangskodetjenesten gøre arbejdet!

En adgangskodetjeneste opretter, gemmer og udfylder automatisk dine adgangskoder. Så skal du kun huske én adgangskode: koden til selve adgangskodetjenesten.

Når vi bruger stærke adgangskoder, gør vi det sværere for kriminelle at stjæle vores:

Data

Identitet

Penge

Opret lange adgangskoder

Mindst 16 tegn, jo længere jo stærkere!

Opret tilfældige adgangskoder

Der er to måder at gøre dette på:

1. Brug en tilfældig række af bogstaver (store og små), tal og symboler (det stærkeste valg). Eksempel: cXmnZK65rf*&DaaD

2. Lav en huskevenlig sætning med 5-7 ord, der ikke har nogen forbindelse til hinanden. Eksempel: ButikLøblGranskoven

Bemærk: Vær lidt kreativ med stavningen, så bliver adgangskoden stærkere.

Lav unikke adgangskoder

Brug forskellige adgangskoder til hver konto, du har:

Eksempel:

- k8dfh8c@Pfv0gB2
- LmvF%swVR56s2mW
- e246gs%mFs#3tv6