Tips og råd

Få gode sikkerhedsvaner på internettet med disse tips og råd. Denne sektion er udviklet i samarbejde med Get Safe Online (Det Forenede Kongerige) og Department of Homeland Security (USA).

- Beskyt din pc og dine bærbare enheder
- Beskyt dine personlige oplysninger og din identitet
- Beskyt forretningsoplysninger uden for din organisation
- Gå på internettet med forsigtighed
- Brug internettet med omtanke

Beskyt din pc og dine bærbare enheder

Pc

- Brug en firewall: Firewalls beskytter dit netværk mod en del vira og hackere.
- Installer antivirussoftware: Antivirussoftware beskytter mod, at virusinfektioner spredes på din computer.
- Få de seneste sikkerhedsopdateringer: Hold dine applikationer og dit operativsystem intakt og opdateret.
- Stop spyware: Undgå mistænkelige e-mails og vedhæftede filer for ikke at lade fremmede komme ind i din computer.
- Tag backup regelmæssigt: Beskyt dine data mod en nødsituation.

Bærbare computere

- Luk for trådløse forbindelser, der ikke er i brug eller nødvendige.
- Tilslut regelmæssigt din bærbare computer til et netværk, du har tillid til, for at opdatere dine sikkerhedsmekanismer.
- Tag backup af dataene på din bærbare computer.
- Efterlad ikke din bærbare computer uden opsyn.

USB-drev

- Anvend et krypteret USB-drev.
- Anvend USB-flashdrevet i skrivebeskyttet tilstand for at undgå overførsel af virus: Enkelte USB-flashdrev har en fysisk knap til at sætte drevet i skrivebeskyttet tilstand for at undgå, at værtscomputeren skriver på drevet eller ændrer dataene.
- Scan USB-flashdrevet efter kopiering af filer fra en upålidelig og/eller uautoriseret computer for at undgå overførsel af virus.

- Inden USB-drevet indsættes i en anden persons computer, slet alle filer, der ikke er relevante for den pågældende handling.
- Tag backup af dataene på dit USB-drev for at kunne genoprette dataene i en nødsituation.
- Sæt USB-drev i nøgleringe/-snore for ikke at tabe dem: På grund af USB-flashdrevenes lille størrelse er det lettere at tabe dem, eller de kan lettere blive stjålet. Desuden øger den større lagringskapacitet den datamængde, der potentielt risikerer at blive udsat for uautoriseret adgang. USB-flashdrev opbevares sædvanligvis i tasker, rygsække, computertasker, jakke- eller bukselommer eller efterlades uden opsyn på arbejdspladsen. Antallet af hændelser er i den seneste tid steget, da USB-drev i stigende grad mistes, forlægges, lånes uden tilladelse eller stjæles.

Mobiltelefoner og håndholdte computere

Håndholdte computere såsom Windows Mobile-, Palm-, iPhone-, Android- og Blackberry-enheder har internetforbindelse og er i stand til at lagre enorme mængder information. Selve deres portabilitet betyder, at omgangen med dem kræver ekstra forsigtighed.

- Luk for trådløse forbindelser (dvs. Bluetooth og WLAN), der ikke er i brug. Ved hjælp af Bluetooth-teknologi kan elektroniske enheder kommunikere indbyrdes via en kortrækkende radioforbindelse.
- Efterlad ikke din mobiltelefon og håndholdte computer uden opsyn. Du risikerer i modsat fald at miste data.
- Anvend passwordfunktionen til at forhindre hacking af din smartphone.

Beskyt dine personlige oplysninger og din identitet

- **Brug et stærkt password**: Dit password svarer til låsen og nøglen til dit hus på internettet. Passwords er en vigtig beskyttelse, og en god praksis i forbindelse med passwords vil hjælpe med til bedre at beskytte dine følsomme personlige oplysninger og din identitet. Passwordet til din computer giver adgang til alle oplysninger — både virksomheds- og personoplysninger — som du har lagret på din computer og dine onlinekonti. Brug et stærkt password til at beskytte dine data: Brug et kompleks sæt af tegn, og kombiner bogstaver (store og små), tal og symboler. Jo større variation i tegnene, du bruger i dit password, desto sværere er det at gætte. Brug ikke personlige oplysninger — dit navn, dit barns navn, fødselsdage osv. — som nogen måske allerede kender, eller som er lette at få fat i, og forsøg at undgå almindelige ord, da nogle hackere anvender programmer, som forsøger at anvende ethvert ord, der findes i ordbogen.
- **Skift dit password regelmæssigt**: Hvis du tror, at nogen uretmæssigt har haft adgang til dit system, så skift passwords øjeblikkeligt.
- **Hold dit password hemmeligt**: Dit password er unikt og må ikke deles med nogen. Forsøg så vidt muligt at indprente dig dine passwords. Hav en strategi til at huske dem udenad.

Hvis du skriver dine passwords ned, så opbevar dem et sikkert sted. Opbevar kun dine passwords på steder, hvor du ville opbevare de oplysninger, de beskytter.

- **Unik konto, unikt password**: Brug et forskelligt password til hver onlinekonto, du anvender (eller i det mindste flere forskellige passwords). Hvis du bruger det samme password til flere konti, vil en angriber, der får adgang til den ene konto, kunne få adgang til alle dine konti.
- **Sørg for at sikre dine konti**: Mange udbydere af konti tilbyder yderligere måder til at verificere, hvem du er, inden du udfører forretninger på det pågældende websted.
- **Styr selv din færden på internettet**: Når det er muligt, så sæt privatlivs- og sikkerhedsindstillingerne på websteder på det niveau, hvorpå du ønsker at dele oplysninger. Det tilrådes at begrænse, hvem du deler oplysninger med.
- **Vær forsigtig, når du bruger sociale netværkssteder**: Vær opmærksom på, at sociale netværkssteder kan omfatte mange af de risici, der er forbundet med at være på internettet: internetmobning, offentliggørelse af private oplysninger, cyberstalking, adgang til ikke-alderssvarende indhold og – mest ekstremt – onlinegrooming og misbrug af børn.

Beskyt forretningsoplysninger uden for din organisation

- **Sørg for at opbevare følsomme oplysninger sikkert**: Når du befinder dig uden for din organisation, så sørg hele tiden for at opbevare følsomme oplysninger og udstyr sikkert for at undgå tyveri eller tab. Vær navnlig forsigtig med håndtering af oplysninger, når du befinder dig på offentlige steder.
- **Hold forretningsoplysninger fortrolige**: Vær opmærksom på, at andre kan overhøre din samtale. Gør ikke din organisations fortrolige oplysninger tilgængelige for enhver.
- **Vær opmærksom på kig-over-skulderen**: Når du rejser eller arbejder fra en decentral arbejdsplads, så beskyt dig mod, at nogen kigger dig over skulderen.
- **Brug webmail med omtanke**: Det kræver samme forsigtighed at bruge en internetbrowser til at læse din post som et desktoppostsystem, og det er forbundet med nogle specifikke sikkerhedsrisici.

Gå på internettet med forsigtighed

- **Luk for trådløse forbindelser, der ikke er i brug eller nødvendige.**
- **Brug Wi-Fi-hotspots med omtanke**: Ved brug af Wi-Fi-hotspots bør du begrænse den form for forretninger, du udfører, og tilpasse sikkerhedsindstillingerne på din enhed for at begrænse, hvem der kan få adgang til din computer.
- **Beskyt dine penge**: Når du udfører bankforretninger eller shopper på internettet, så kontroller, at webstederne er sikkerhedsaktiverede. Se efter internetadresser med "https://" eller "shttp://", hvilket betyder, at der på webstedet er truffet ekstra foranstaltninger til at beskytte dine oplysninger. "Http://" er ikke sikker.
- **Stop uønsket e-mail**: Spammail er en sikkerhedstrussel. Åbn ikke ukendte e-mails og vedhæftede filer.

- **Hvis du er i tvivl, så slet dem**: Når links i e-mails, tweets, opslag og onlinereklamer ser mistænkelige ud, er det bedst at slette dem eller eventuelt markere dem som junkmail, selv om du kender kilden.
- **Videresend e-mails, når det er nødvendigt**. Overvej dog først at slette meddelelseshistorien.
- **Vær forsigtig, når du færdes på internettet.**
- **Download ikke dokumenter og materiale fra usikre kilder.**
- **Vær forsigtig, når du bruger offentlige computere:** Gå kun på internettet på en offentlig computer, når du har en krypteret forbindelse (markeret ved en hængelås nederst i højre side af dit browservindue og ved bogstaverne "https://" i begyndelsen af internetadressen).
- **Brug webmailtjenester fra velkendte virksomheder, du har tillid til.**

Brug internettet med omtanke

- **Hold dig opdateret:** Hold dig ajour med nye måder til at tage vare på sikkerheden på internettet: Find de seneste oplysninger på websteder, du har tillid til, og del disse oplysninger med familie, venner og kollegaer, og tilskynd dem til at bruge internettet med omtanke. Gør din browser sikker.
- **Tænk, før du handler**: Vær forsigtig med meddelelser, der opfordrer dig til at handle øjeblikkeligt, tilbyder noget, der lyder for godt til at være sandt, eller beder om personlige oplysninger.
- **Tag backup**: Beskyt dit arbejde, din musik, dine fotos og anden digital information ved at lave en elektronisk kopi og opbevare den sikkert.