|  |
| --- |
| God digital adfærd |
|  |
| Leveregler for Virksomhed |
| **Eksempel**Oplysninger om personer har en værdi som aldrig før, og den digitale udvikling har gjort, at adgang til personoplysninger i stort omfang er så nemt som aldrig før. Det koster eksempelvis helt ned til blot 12 kroner at købe et såkaldt DDoS-angreb på en hjemmeside, eller 1 EUR at købe 2 millioner e-mailadresser. Hos Virksomhed vil vi gøre os umage med at passe på menneskers personlige oplysninger. Derfor er det vigtigt, at vi gør hvad vi kan for at beskytte dem mod at uvedkommende får adgang til dem.Uvedkommende har mange kasketter. Det er professionelle hackere eller it-kriminelle, der via ransomware kan kryptere alle vores data og tage dem som gidsler for en normalt betydelig løsesum. Men uvedkommende er også kollegaer, familie og bekendte, som ikke i deres arbejde eller af anden fornuftig grund skal have adgang til andre menneskers personlige oplysninger. I vores omgang med personlige oplysninger er det derfor lige så vigtigt, at vi naturligvis beskytter os med udefra kommende indgreb, men at vi også i vores daglige arbejde respekterer privatlivet og ikke deler personoplysninger, som vi får adgang til via vores arbejde. Sikkerhed på arbejdspladsen er alles ansvar, og ikke kun it-afdelingens. En enkelt fejl eller ubetænksomhed hos en medarbejder kan skade hele vores it-system og vores samarbejdspartnere, lejere mv.’s tillid. Denne politik udgør Virksomheds leveregler for god digital adfærd.  |

|  |
| --- |
| Generelle leveregler |
| #1 | Opdater al software – udover at introducere nye lækre funktioner, indeholder en opdatering altid leverandørens tiltag til at beskytte systemerne og lukke eventuelle huller.  |
| #2 | Vær varsom med, hvad du tilslutter til computeren – USB-nøgler eller andre enheder, kan være smittede med virus og malware, og kan smitte din computer, og i værste tilfælde hele Virksomheds it-systemer og netværk. Undlad at bruge USB-nøgler til at flytte data, og tilslut kun USB-nøgler, hvor du har tillid til den person/virksomhed, du har fået den fra. |
| #3 | Vær varsom med dine fortrolige oplysninger og virksomhedens oplysninger. Undlad at indtaste private oplysninger eller særlige virksomhedsoplysninger på sociale medier, og lad helt være med at indtaste dem på netværk eller enheder, som ikke er dine egne eller virksomhedens.  |
| #4 | Brug stærke adgangskoder – et godt kodeord er langt og gerne med brug af tal, store/små bogstaver og specialtegn. Brug aldrig det samme kodeord flere steder. Undlad at dele dit kodeord med andre. Brug eventuelt en password-manager. Eksempelvis kan www.lastpass.com bruges.  |
| #5 | Vær sikker på, hvem du kommunikerer med. Er du den mindste smule usikker, skal du ignorere e-mailen/sms’en og forsøge at få bekræftet henvendelsen på anden måde, eksempelvis ved at ringe til den pågældende. Det er IKKE flovt at spørge om identitetsbekræftelse.  |
| #6 | Beskyt dine og virksomhedens oplysninger mod ransomware – åbn aldrig vedhæftninger eller links fra ukendte afsendere, eller afsendere, hvor du er usikker på, om afsenderen er den, vedkommende siger, at han er. Se under #4.  |
| #7 | Færrest mulige brugere skal have rettigheder til hardware og software. Hver bruger skal kun have adgang til de oplysninger, som den pågældende har brug for, for akkurat at kunne udføre sit arbejde. Det betyder færrest mulige brugerrettigheder. Der kan derfor være en god grund til, at du ikke har adgang til det samme som din kollega.  |
| #8 | Kig efter s’et (HTTPS) – hjemmesider, der kommunikerer via ”http” mangler sikkerhed, og it-kriminelle kan lytte med. ”HTTPS” er en krypteret og dermed sikker måde at kommunikere på via internettet. Du skal derfor sikre dig, at der i din browsersti øverst (URL) står https foran web-adressen eller at der er en grøn hængelås. |

Generelle leveregler, fortsat

|  |  |
| --- | --- |
| #9 | Undgå at bruge offentlige netværk – du vil blive overrasket over, hvor meget andre kan ”lytte” med på din kommunikation. Du kan heller ikke være sikker på, at du rammer det offentlige netværk – it-kriminelle kan have opsat en router, der næsten hedder det samme, så når du tror du har logget dig på et offentligt netværk, er det i virkeligheden de it-kriminelles netværk. Brug i stedet din mobiltelefon som router eller få hjælp fra it-afdelingen til at få installeret en VPN-forbindelse, du kan bruge på offentlige netværk. Arbejder du hjemmefra skal du sørge for at ændre password til din egen router, så det ikke er det password, der ”fulgte med”. Har du brug for hjælp til det, kan du ringe til din teleudbyder eller spørge it-afdelingen.  |
| #10 | Undlad at installere applikationer uden tilladelse fra it-afdelingen – applikationer kan bruges til at lagre mange flere oplysninger om dig, end de reelt har behov for. Særligt hvis de er gratis.  |
| #11 | Spamfilteret er installeret af en årsag – undlad at åbne mails, der ligger i spamfilteret, medmindre du er helt sikker på, at afsenderen og e-mailen er troværdig. |
| #12 | Undlad at ændre på indstillinger, eksempelvis at Flash Player skal aktiveres manuelt.  |
| #13 | Lås altid dine enheder, når du forlader dem – og undlad i det hele taget at efterlade dem uden opsyn på steder med offentlig adgang.  |
| #14 | Dobbelttjek oplysninger fra udefrakommende – får du en henvendelse fra en myndighed, virksomhed, organisation, advokat, revisor eller andre, der vil have dig til at gøre noget for sig, skal du altid dobbelttjekke oplysningerne – tjek virksomheds­oplysninger, tegningsberettigede personer mv. via forskellige databaser, eksempelvis via CVR-numre. Er du stadig i tvivl, kan du ringe og få bekræftet, at henvendelsen er fra den, som den giver sig ud for at være.  |
| #15 | Brug din sunde fornuft – hvis noget lyder for godt til at være sandt, så er det typisk også. |