telecentre danmark

NetsikkerNu!

- med sund fornuft når man langt

Gode råd om sikkerhed på nettet

PC, tablets, smartphone

://getonlineweek.eu

get empowered,
get employed

Gode råd om It-sikkerhed
- Beskytter dig selv og andre og pas på dine personlige oplysninger.

En vedligeholdt computer beskytter:
1. Brug et antivirusprogram med automatisk opdatering, en firewall og et antispyware program.
2. Anvend altid opdaterede versioner af dit styresystem, din webbrowser og dit e-mailprogram m.v Slå automatisk opdatering til, hvor det er muligt, så glemmer du det ikke.
3. Hvis du benytter trådløst internet/WI-FI, så slå kryptering til – ellers kan andre kigge med og evt. misbruge din internetforbindelse.
4. Indstil sikkerhedsniveauet i din browser, så du altid bliver spurgt, når informationer, filer og programmer overføres til din computer.
5. Bruger du fx Facebook, så husk at tage stilling til "privacy": hvem må se dine opslag mv.

Du kan selv gøre meget:
1. **Brug adgangskode** til log-in på din computer og mobile enheder. Adgangskoder er den vigtigste beskyttelse af dine personlige oplysninger. Lav derfor en sikker adgangskode, dvs. en kode på mindst 8 tegn med tal, bogstaver og specialtegn.
2. Vær ekstra opmærksom, når du åbner **vedhæftede filer.** De kan indeholde virus. Pas især på filer med underlige eller lokkende navne. Også selvom de kommer fra nogen, du kender.
3. Brug din sunde fornuft, eller bed andre om hjælp, hvis du er i tvivl. Selv om du har både antivirusprogram, firewall og antispywareprogram, skal du forholde dig kritisk til de netsteder, du besøger.
4. Vær påpasselig med at skrive personlige oplysninger i **e-mail**. En e-mail er i princippet lige så tilgængelige som et åbent postkort. Hvis du sender fortroligt materiale i en e-mail, så brug kryptering. Hold øje med om netsteder, der beder om fortrolige oplysninger, benytter kryptering (se efter hængelås i browseren).
5. Slet spam uden at åbne det. Benyt eventuelt et **spamfilter**.
6. Hent kun programmer fra netsteder, du stoler på. Undersøg om du skal afgive private oplysninger og/eller siger ja til reklamer, før du installerer. Vær især opmærksom over for **fildelingsprogrammer og gratis programmer.**
7. **Undgå spyware** og adware. Det er programmer, som opsamler oplysninger om din identitet og adfærd samt udsætter dig for uønsket annoncering mv. De gør samtidig din computer langsommere. Spyware bliver typisk installeret i det skjulte, hvis du klikker på lokkende tekst eller billede ol.
8. Slet e-mail fra banker og betalingstjenester, hvis de indeholder links, du skal klikke på. Du skal heller ikke reagere, hvis e-mailen anmoder dig om personlige og fortrolige oplysninger. Det kan være forsøg på "phishing", en form for svindel, hvor der linkes til falske kopier af netsteder, som du har tillid til.
9. Vær påpasselig, når du bruger **Facebook,** chat og instant messaging. Disse tjenester kan også sprede sikkerhedsproblemer. Vær derfor særligt opmærksom, og **klik kun på links**, hvis **du kan gennemskue,** hvor de fører hen, og du har tillid til afsenderen, og selv da kan der ske fejl– ikke alle opfører sig lige fornuftigt på nettet.
10. **Tænk** over hvad du offentliggør på nettet. Det ligger der til "evig tid".

Inden uheldet er ude:
Lav sikkerhedskopier af dine vigtige dokumenter og filer. Gem dem fx på en USB-nøgle, i skyen på Dropbox , OneDrive o.l Husk at tjekke om de kan genindlæses!

Gode råd om sikker e-handel

1. I forhold til sikkerhed og dine rettigheder er det en fordel at betale med **betalingskort/MobilePay** og helst ikke via en bankoverførsel. Har du betalt med betalingskort, kan banken, hvis varen ikke dukker op, tilbageføre pengene til din konto.
2. Når du betaler med betalingskort på nettet, skal du **kun** oplyse kortnummer, udløbsdato og den 3-cifrede sikkerhedskode, der står bag på kortet.
3. Afgiv aldrig betalingskortoplysninger via e-mail og **afslør aldrig** pinkoden til dit betalingskort.
4. Afgiv kun personlige oplysninger som navn, adresse og telefonnummer, når der er et logisk behov for det, eksempelvis ved bestilling af en vare, der skal fremsendes.
5. Vær særlig kritisk, hvis sælger beder om oplysninger, sælger som hovedregel ikke har behov for, fx CPR- nummer. Se fx de gode råd fra Forbrugerrådet TÆNK på http://taenk.dk/gode-raad/tema/beskyt-dit-cpr-nummer/hvem-maa-bede-om-dit-cpr-nummer.
6. **Forhold dig kritisk**. Er tilbuddet for på nettet er for godt til at være sandt?
   På danske hjemmesider kan du kigge efter **e-mærket**. Netbutikker med e-mærket er godkendt og kontrolleret ,og skal leve op til en række krav. Her kan du også klage, hvis noget går skævt.
   På Hjemmesiden **trustpilot.dk** kan brugerne give deres vurdering af, hvor godt og sikkert et firma er. Dog kan du ikke stole på, at du ser alle dårlige anmeldelser.
7. Undersøg, om forbindelsen på betalingssiden er sikker, når du skal betale. Se derfor efter en **hængelås** eller **https** i din browser, der betyder, at betalingsoplysningerne ikke kan læses af andre.

Vær opmærksom på, at hvis du køber varer af andre privatpersoner, fx på et online brugtmarked, og overfører penge direkte til sælgeren, gælder der andre (ingen) regler.

Betaling via smartphones:

MobilePay der er udviklet af Danske Bank. De fleste banker er med i MobilePay. Betalinger med MobilePay svarer til betaling med Dankort, og sikkerheden og forbrugerbeskyttelsen er således den samme. MoliePay er beskyttet af en selvvalgt 4 cifret koder. Telefonen bør ligeledes sikres af en adgangskode. Det er vigtig også at installere en antivirus app der sikrer telefonen.

Det kontaktløst dankort på mobiltelefonen.

Nets står for udviklingen af det mobile Dankort (på smartphonen). Denne løsning vil både dække smartphones med aktiv Near Field Communication (NFC) og Apple telefoner, hvor brugeren ikke har adgang til NFCfunktionaliteten i telefonen. Når der ikke er adgang til at bruge NFC anvendes QR koder eller Bluetooth.

Betalingen udføres ved at holde mobilen hen til den kontaktløse betalingsterminal uden der behøver at være fysisk kontakt mellem de to enheder. Terminalens display vil fortælle, når betalingen er gennemført. Dankortet på mobilen svare til betaling med det fysiske Dankort, og sikkerheden og forbrugerbeskyttelsen er således den samme.

Phishing og Smishing—Nysgerrighed kan koste dyrt.

Phishing er et svindelforsøg, der går ud på at lokke oplysninger ud af modtageren. Ved phishing modtager du en e-mail, der tilsyneladende er fra en kendt afsender, fx din bank. I mailen er der et link, du kan klikke på, og derefter bliver man bedt om at oplyse fx brugernavn og password mv. Ved at køre musen hen over –**uden at klikke**—kan du se linkets adresse og derved se, om det fører tilbage til den afsender, den udgiver sig fra at komme fra.

Smishing rammer **mobiltelefoner** og går ligeledes ud på at fiske brugernavn og password samt evt. nøglekort fra modtageren. Modtager du derfor en sms med opfordring til at udfylde en formular, sende et billede af dit nøglekort mv. skal du derfor blot slette sms´en. NemID vil aldrig henvende sig til brugeren på denne måde. Din konto lukkes ikke, derimod bliver du udsat for **identitetstyveri.**

5 gode råd til sikkerhed på smartphone og tablet

1. Undgå farlige apps

Se dig for, når du søger efter en populær app. Er den udgivet af det rigtige firma? Hvor længe har den været tilgængelig? Se anmeldelserne før du henter app'en

2. Brug antivirus

Installerer du et antivirusprogram på din mobile enhed, kan det beskytte dig mod de mest udbredte og skadelige apps. Programmet genkender og fjerner de farlige apps.
Antivirus-apps findes både i gratis og kommercielle versioner.

3. Tag kopi af data

Mister du din smartphone eller tablet, mister du samtidig de billeder og kontakter, du har gemt på enheden.

4. Beskyt dig mod at andre får kendskab til dine kodeord mv.

Passwords, kontonumre og andre fortrolige oplysninger er i fare for at blive "aflyttet", hvis du tilkobler dig et åbent netværk.
Brug kun netværk, der er beskyttet med adgangskode – helst med den nyeste teknologi.

5. Brug en pinkode

Så uvedkommende ikke kan komme ind på din telefon.
Krypterer du dine data, når de gemmes, kan du beskytte dem yderligere. Så kan man nemlig kun læse dem, hvis man kender koden.

Husk, at apps kan være gratis, fordi udbyderne tjener pengene på at videresælge dine private oplysninger.

Telecentre-danmark

Telecentre-danmark er en NGO non profit organisation, der tilbyder et netværk for datastuer og andre uformelle undervisningssteder for it-svage borgere. Undervisningssteder der har til formål at understøtte "it-svage" gruppers muligheder for at erhverve og udvikle digitale kompetencer i fællesskab med andre.
Gennem Telecentre-danmarks netværks udvikler datastuerne ny viden, udveksler erfaring mv. til glæde for brugerne.
Datastuer og andre uformelle undervisningssteder modvirker, at for mange ældre, udsatte og andre it-svage borgere ekskluderes fra samfundet

Telecentre-danmark er landsdækkende. Bestyrelsen og medarbejderne har mere end 20 års erfaring med at organiserer frivilligt arbejde og uformel IT undervisning.

Gennem erfaringer fra arbejdet med nationale og internationale projekter og med netværket, arbejder Telecentre-danmark på det politiske niveau for at sikre IT-svage borgere bliver hørt.

Alle har ret til IT—godt for den enkelte—godt for samfundet.

www.tc-danmark.dk **mail: info@tc-danmark.dk** **Telefon +45 311 311 66**

Marts 2017