Gode råd om sikker brug af internettet

Hvad kan vi gøre for dig

Sydbank

Sikker brug af internettet

Ved at være opmærksom på nogle få grundlæggende forhold, når du surfer på internettet eller modtager e-mail, kan du gøre meget for, at andre ikke får adgang til din computer, eller at du ikke modtager virus og lignende.

Du bør derfor læse følgende gode råd, inden du bruger Online Banking/NetBank:

1. Undlad at klikke på links og at åbne vedhæftede filer i e-mails, hvis du er i tvivl om indholdet. Vær især kritisk overfor uopfordrede e-mails og e-mails fra ukendte afsendere. Vær ekstra forsigtig, når uopfordrede e-mails har links og vedhæftede filer – lad være med at klikke på disse.

   Det samme gælder phishing-e-mails, hvor du opfordres til at udlevere personlige data. Ofte udgiver e-mailen sig for at være afsendt fra fx en bank, fra Nets, SKAT eller Visa. I mange tilfælde indeholder den et link – men klikker du på det, giver du hackeren mulighed for at angribe din computer. Slet e-mailen og lad være med at klikke på de vedhæftede filer eller links.

2. Opdater altid browser, e-mail-program, hjælpeprogrammer og operativsystem, så du altid har de nyeste versioner og dermed også har de nyeste sikkerhedsopdateringer.

3. Brug altid et opdateret antivirusprogram, der automatisk tjekker filer, e-mails m.m., før de lagres.

4. Når du kommunikerer sikkert over internettet, kan du se en hængelås enten nederst til højre eller øverst i browseren. Klik på hængelåsen for at få vished om, hvem du kommunikerer med.

5. Forvis dig om, at virksomhedens it-udstyr og netværk er beskyttet af en opdateret firewall.

6. Indstil browseren således, at den giver en advarsel, før noget downloades til pc'en. Acceptér kun download fra sites/kilder, som du kender og finder troværdige. Tjek certifikatet – se punkt 4.

7. Vælg en sikkerhedskode, der er svær at gætte, og hold den hemmelig/personlig. Skift sikkerhedskode med jævne mellemrum.

8. Benytter du trådløst netværk, skal du huske at slå kryptering til. Kontakt evt. din it-leverandør eller teleudbyder.

9. Anvend kun Online Banking/NetBank på maskiner, du har tillid til. Og husk altid at logge rigtigt af.

10. Har andre adgang til dit netværk via fjernskrivebord, så skal denne adgang være begrænset mest mulig med godkendelse af IP-adresse og sikkerhedskode.

Nyeste information finder du på login-siden til Online Banking og NetBank.

Hvem dækker misbrug af konti i Online Banking/NetBanken?

Har Online Banking eller din NetBank været udsat for indbrud af it-kriminelle, gælder der forskellige regler for, hvem der hæfter for eventuelt tab. Det afhænger af kontotypen (privatkonto eller erhvervskonto).

Privatkonti

Er der sket misbrug af privatkonti, og brugeren har udvist normal adfærd, er det som udgangspunkt banken, der dækker eventuelt tab.

Privatkonti, der bruges til erhvervsbetalinger, betragtes som erhvervskonti.

Erhvervskonti

For erhvervskonti er der ikke samme dækning som for privatkonti. Dette betyder, at det er virksomheden selv, der skal dække et tab ved indbrud på erhvervskonti.

Beskyt dig mod tab som følge af misbrug af erhvervskonti

Selvom virksomheden har klare forretningsgange, der sikrer it-systemerne, kan der ske indbrud, fx hvis en medarbejder åbner en e-mail, hjemmeside eller downloader et program, der er inficeret med virus, spyware eller lignende. Vi anbefaler, at I tegner en forsikring mod tab som følge af uberettiget anvendelse. Kontakt evt. virksomhedens forsikringsselskab eller revisor for at høre nærmere om mulighederne.

Har du mistanke?

Har du klikket på en mistænkelig e-mail, eller har du mistanke om virus på din pc, skal du undgå at logge på Online Banking/NetBank og straks kontakte Sydbanks Hotline for at få Online Banking/NetBank spærret. Anvender du Sydbank Online Banking, skal du ringe til Sydbanks Hotline på 74 37 25 10. Anvender du Sydbank NetBank, skal du ringe til Sydbanks Hotline på 74 37 25 98. Udenfor åbningstiden kan du kontakte Spærreservice på 75 94 50 93.

sydbank.dk

Sydbank

154440315