Gode råd om nethandel
8 tip til mere sikkerinternethandel

Beskyt dig selv og computeren, når du handler på internettet
Sikkerhedstrusler online forekommer i dag som angreb mod din computer og dine personlige oplysninger. Her er otte tip til at gøre handel på internettet mere sikkert for dig:

1. Hold computerens software opdateret.
Hold al software (inklusive webbrowseren) opdateret med automatiske opdateringer. Du kan sikre dig dette med programmet Secunia, som du kan finde under Link til programmer

2. **Beskyt computeren**.
Installer firewall-, antivirus-, antispam- og antispywareprogrammer. Du kan give computerens sikkerhed et ekstra beskyttende lag ved at hente Microsoft Security Essentials gratis eller vha. andre antivirus -programmer.

3. Undgå malware og forsøg på phishing.

Internet Explorer 8 bruger som udgangspunkt SmartScreen-filteret til at blokere og advare dig mod skadelig kode og forsøg på phishing. SmartScreen-filteret viser en advarsel, hvis en given webside er rapporteret som usikker, og du har samtidig mulighed for selv at rapportere usikre websider.

4. Beskyt dig selv mod nye trusler

Scriptangreb på tværs af websider er en af de stadig mere avancerede metoder, som it-kriminelle bruger til at få fat i dine personlige oplysninger. Internet Explorer 8 er med til at beskytte dig mod sådanne angreb vha. et XSS-filter (Cross Site Scripting), der som udgangspunkt altid er aktiveret.

5. Identificer falske websteder.

Med Internet Explorer kan du bedre undgå at falde i fælden på websteder, der forsøger at narre dig med vildledende adresser. Domænenavnet fremhæves med sort på adresselinjen, så det bliver nemmere at identificere webstedets virkelige identitet.

6. Mere privat surfing på internettet.

Når du bruger en offentlig computer til at læse e-mail eller en delt pc til at købe en gave som en overraskelse, er det en god idé at bruge InPrivate-browsing – en funktion, der gør det let for dig at skjule, hvilke sider du har besøgt, cookies og andre oplysninger for andre brugere af samme computer.

7. Kontroller, at webstedernes betalingssystem bruger datakryptering.

Hold øje med følgende tegn på, at et websted bruger kryptering af kreditkortoplysninger og lignende:
§ Der er et s i webstedets adresse – dvs. adressen starter med https:
§ En lille, lukket hængelås på adresselinjen eller i nederste, højre hjørne af vinduet.
§ En grøn adresselinje i Internet Explorer 8 betyder, at webstedet er sikkert.

8. Svar aldrig på uopfordrede anmodninger om at opdatere dine kontooplysninger.

Sådanne e-mail kan være forklædte henvendelser fra nogen, der forsøger at franarre dig dine personlige oplysninger. De fleste legitime virksomheder sender aldrig uopfordret e-mail eller andre meddelelser, hvori de opfordrer dig til at udlevere adgangskoder eller andre personlige oplysninger. Husk desuden, at hvis noget lyder for godt til at være sandt, er det sikkert også tilfældet.