Tips & råd

Dessa tips och råd hjälper dig att använda internet på ett säkert sätt. Avsnittet har utarbetats i samarbete med Get Safe Online (Storbritannien) och Department of Homeland Security (USA).

- Skydda din persondator (pc) och dina bärbara enheter
- Skydda dina personuppgifter och din identitet
- Skydda affärsinformation utanför din organisation
- Koppla upp dig klokt
- Var nätsmart

Skydda din persondator (pc) och dina bärbara enheter

Pc

- Använd en brandvägg: brandväggar skyddar ditt nätverk mot en del virus och hackare.
- Installera antivirusprogram: antivirusprogram hindrar virus från att sprida sig i din dator.
- Hämta de senaste säkerhetsuppdateringarna: håll dina program och operativsystem friska och uppdaterade.
- Stoppa spionprogram: se upp för misstänkta e-postmeddelanden och bilagor så att inte främlingar tar sig in i din dator.
- Säkerhetskopiera regelbundet: skydda din dator mot katastrofer.

Bärbara datorer

- Stäng av trådlösa anslutningar när de inte används eller behövs.
- Anslut regelbundet din bärbara dator till ett nätverk du litar på för att uppdatera dina säkerhetsmekanismer.
- Säkerhetskopiera de uppgifter som finns lagrade i din bärbara dator.
- Lämna inte din bärbara dator utan tillsyn.

USB-minnen

- Använd ett krypterat USB-minne.
- Använd kontakten för att försätta USB-minnet i skrivskyddat läge så att du undviker virus. Vissa USB-minnen har en fysisk kontakt för att försätta minnet i skrivskyddat läge så att värddatorn inte kan skriva till minnet eller ändra data som ligger på det.
- Sök igenom USB-minnet när du kopierat filer från en obehörig maskin eller en maskin du inte litar på så att du undviker virus.
- Radera alla onödiga filer innan du sätter ditt USB-minne i någon annans dator.

- Säkerhetskopiera informationen på ditt USB-minne så att du kan återskapa data vid en katastrof.
- Fäst USB-minnen vid nyckelringar eller nyckelband för att undvika förlust. Eftersom USB-minnen är så små kan de lätt komma bort eller bli stulna. Den stora lagringskapaciteten gör dessutom att en större mängd data kan komma i orätta händer. USB-minnen placeras ofta i väskor, ryggsäckar, datorväskor, jackor eller byxfickor eller lämnas i obevakade arbetsstationer. Det händer allt oftare att USB-minnen försvinner, tappas bort, lånas utan tillåtelse eller blir stulna.

Mobiltelefoner och handdatorer

Handdatorer som Windows Mobile, Palm, iPhone, Android och Blackberry har webblänkar och kapacitet att lagra stora mängder information. Just att de är bärbara betyder att de måste behandlas extra försiktigt.

- Stäng av trådlösa anslutningar (som bluetooth och WLAN) när de inte används. Med hjälp av bluetooth-teknik kan elektroniska enheter kommunicera med varandra genom en radiolänk med kort räckvidd.
- Lämna inte din mobiltelefon och handdator utan tillsyn. Du kan förlora data.
- Använd lösenordsfunktionen för att förhindra intrång i din smarttelefon.

Skydda dina personuppgifter och din identitet

- **Använd ett starkt lösenord**: På internet är ditt lösenord som låset och nyckeln till ditt hus. Lösenord är ett viktigt skydd, och med goda lösenordsvanor är dina känsliga personuppgifter och din identitet säkrare. Lösenordet till din dator är nyckeln till all information – både företags- och personuppgifter – du har lagrat på din dator och på konton på internet. Använd ett starkt lösenord för att skydda dina uppgifter – en invecklad kombination av bokstäver (små och stora), siffror och symboler. Ju fler olika tecken ditt lösenord innehåller, desto svårare är det att gissa. Använd inte personuppgifter – ditt namn, dina barns namn, födelsedagar osv. – som någon kanske redan känner till eller lätt kan ta reda på. Försök också att undvika vanliga ord – en del hackare använder program som provar varje ord i ordboken.
- **Byt lösenord regelbundet**: om du tror att ditt system är utsatt för risk, byt lösenord omedelbart.
- **Håll ditt lösenord hemligt**: Ditt lösenord är unikt och ska inte lämnas ut till någon. Försök att memorera dina lösenord om det går. Hitta en strategi för det. Om du skriver ner dina lösenord, var försiktig med var du förvarar dem. Lämna inte uppgifterna om dina lösenord någonstans där du inte skulle lämna den information de skyddar.
- **Unikt konto, unikt lösenord**: Använd ett lösenord för varje webbkonto du har tillgång till (eller åtminstone flera olika lösenord). Om du använder samma lösenord för flera olika konton kan en angripare som får tillgång till ett konto komma åt alla dina konton.

- **Skydda dina konton**: många kontoförare erbjuder fler sätt att bekräfta din identitet innan du kan göra transaktioner på webbplatsen.
- **Ha kontroll över din närvaro på nätet**: När det finns sekretess- och säkerhetsinställningar på en webbplats, ställ in dem till önskad nivå när det gäller informationsdelning. Var restriktiv med vem du delar information med.
- **Var försiktig när du använder sociala nätverkssajter**: på sociala nätverkssajter förekommer många av de risker som förknippas med internetanvändning – nätmobbning, utlämning av privat information, nätstalkning, tillgång till innehåll som inte lämpar sig för vissa åldrar och, i extremfall, nätgromning och övergrepp mot barn.

Skydda affärsinformation utanför din organisation

- **Se till att känsliga uppgifter är säkra**: Ha alltid uppsikt över känsliga uppgifter och utrustning när du befinner dig utanför din organisation, för att undvika stöld eller förlust. Var särskilt rädd om information när du befinner dig på offentliga platser.
- **Håll affärsuppgifter konfidentiella**: Var medveten om att någon kan höra dina samtal. Låt inte alla få tillgång till din organisations konfidentiella information.
- **Se upp för tjuvsurfande**: skydda dig mot tjuvsurfande när du reser eller arbetar på distans.
- **Använd webbpost klokt**: var lika försiktig när du använder en webbläsare för att läsa din e-post som när du använder ett e-postprogram i din dator, och tänk på de ytterligare säkerhetsriskerna.

Koppla upp dig klokt

- **Stäng av trådlösa anslutningar när de inte används eller behövs.**
- **Var smart när det gäller wi-fi-surfzoner**: var restriktiv med vad du gör när du använder wi-fi-surfzoner, och anpassa säkerhetsinställningarna på din enhet för att begränsa åtkomsten till den.
- **Skydda dina pengar**: När du gör bankärenden och handlar på internet, kontrollera att webbplatserna är säkerhetsskyddade. Leta efter webbadresser med ”https://” eller ”shttp://”. Det betyder att extra åtgärder vidtagits för att skydda dina uppgifter. ”http://” är inte säkert.
- **Stoppa oönskad e-post**: Skräppost är ett säkerhetshot. Öppna inte okända e-postmeddelanden och bilagor.
- **Är du tveksam – radera**: när länkar i e-postmeddelanden, tweets, statusuppdateringar och webbreklam ser misstänkta ut, även om du känner till källan, är det bäst att radera och eventuellt markera som skräppost.
- **Vidarebefordra e-post om det är lämpligt**. du kanske vill radera meddelandehistoriken innan du vidarebefordrar.
- **Surfa försiktigt.**
- **Ladda inte ner dokument och material från parter du inte litar på.**

- **Använd offentliga datorer försiktigt:** koppla bara upp dig på en offentlig dator om du har en krypterad anslutning (du ser ett hänglås längst ner till höger i webbläsarfönstret och webbadressen börjar med ”https://”).
- **Använd webbposttjänster från välkända företag som du litar på.**

Var nätsmart

- **Håll dig uppdaterad:** Häng med i utvecklingen när det gäller internetsäkerhet. Leta efter den senaste informationen på webbplatser du litar på. Berätta för familj, vänner och kolleger och uppmana dem att vara nätsmarta. Se till att din webbläsare är säker.
- **Tänk efter före**: var försiktig med uppmaningar att agera direkt och erbjudanden som låter för bra för att vara sanna eller förfrågningar om personuppgifter.
- **Säkerhetskopiera**: skydda ditt arbete, din musik, dina foton och annan digital information genom att göra en elektronisk kopia och förvara den säkert.