

Digitalisering och datasäkerhet

ALLEGRO INK

I den här serien skriver gästande kolumnister från Allegro Ink. Allegro Ink är en utvecklande gemenskap för projektfolk och företagare i Campus Allegro.

Digitaliseringen, det vill säga framväxten av digitala lösningar i vardagen sker snabbt och ändrar samhället vi lever i. I samtakt med de nya lösningarna har digitaliseringen också skapat nya utmaningar för de som kämpar för datasäkerheten. Det finns risk för dataintrång eller dataförlust varje gång någon bestämmer sig för att klicka på en länk eller öppnar en e-post-bilaga. En oförsiktig slutanvändare kan genom sina åtgärder åstadkomma kolossala skador. Man kan köpa dyra säkerhetsverktyg för att skydda sitt system, men det finns några enkla tips man också kan följa för att förbättra datasäkerheten.

1. Inse till en början att du är ett attraktivt mål för kriminella. Om något kan hända, kan det också hända dig och därför är det bra om du agerar i preventivt syfte.

2. Du har redan tidigare hört att du skall använda dig utav bra lösenord. Gör det. Använd dig av en kombination av siffror, bokstäver, skiljetecken samt specialtecken och



TOM TUUNAINEN

Centria forskning utveckling och innovation

använd inte samma lösenord för alla dina tjänster. Dela inte ditt lösenord med andra, skriv inte ner det och skriv det definitivt inte på en lapp som är klistrad på din bildskärm eller ligger på ditt skrivbord var det lätt kan läsas av.

3. Uppdatera regelbundet ditt datasäkerhetsprogram. För en sån har du väl? Om du inte har en, gå då och skaffa dig en. De kostar inte mycket. Och kom ihåg att, även de

bästa datasäkerhetsprogram inte är till hjälp om du inte håller programmet uppdaterad.

4. Var försiktig med det du klickar på i dina e-postmeddelanden. Länkar och bilagor i meddelandet kan åstadkomma stor skada i fall att de har kommit från skumma källor. Detta gäller också nedladdade filer från webbplatser. Sök alltid igenom filerna med ditt datasäkerhetsprogram. Det minskar sannolikheten för att din dator blir infekterad. Kontrollera också noga adressen på webbplatsen som länken tar dig till. Kriminella använder sig ofta av förvrängningar av något som påminner om riktiga platser för att leda dig till något skadligt.

5. Var också försiktig med vad du ansluter till din dator. Skadlig programvara kan sprida sig via smittade externa minnen, hårddiskar och till och med via din mobiltelefon. Sök alltid igenom det du anslutit till din dator med ditt datasäkerhetsprogram.

6. Om du behöver lämna din dator, telefon eller surfplatta, läs den så att ingen kan använda den till något du inte vill medan du är borta.

7. Känn till att det data du överför via

”Kom dessutom också ihåg det gamla goda rådet att regelbundet ta säkerhetskopior av det du anser är viktigt.”

nätet väldigt lätt kan kopieras eller stjälas. Därför är det viktigt att du handlar eller går till nätbanken endast på en dator, telefon eller surfplatta som tillhör dig eller du är helt säker på och dessutom på ett nätverk som du litar på.

8. Kom dessutom också ihåg det gamla goda rådet att regelbundet ta säkerhetskopior av det du anser är viktigt. I fall att något sker har du då det viktiga i behåll.

Diskutera gärna dessa tips med dina nära och kära. Har alla generationer i familjen koll på att t.ex. en nedladdad fil kan vara ett program som kan göra oönskade ändringar på hemdatorn?

Behöver du hjälp med dessa samt andra datasäkerhetsfrågor kan du vara i kontakt med din leverantör av datasystem.

Centria yrkeshögskola kan också vara till hjälp i datasäkerhetsfrågor. Yrkeshögskolan har bl.a. påbörjat ett datasäkerhetsprojekt med namnet SecuBot vars mål är att bygga ett laboratorium i Campus Allegro i Jakobstad för att skapa nya färdigheter som tjänar regionens företag samt att höja nivån på datasäkerheten i hela Österbotten.