DELL Technologies

Cybersäkerhetsfusklapp

I vår alltmer virtuella värld är det kanske inte konstigt att cyberbrott blir allt vanligare. Faktum är att **cyberbrott genererade runt 6 biljoner dollar 2021**, vilket gör det till världens tredje största ekonomi efter USA och Kina!* Angripare blir smartare och mer sofistikerade för varje dag som går, men det är lätt att vara säker online om man känner till de senaste hoten och har rätt säkerhetsåtgärder på plats. **Här följer några exempel på hot som Dells cybersäkerhetsexperter arbetar hårt för att förhindra och tips på hur du kan skydda din arbetsplats och ditt hem.**

Oväntade kompromisser

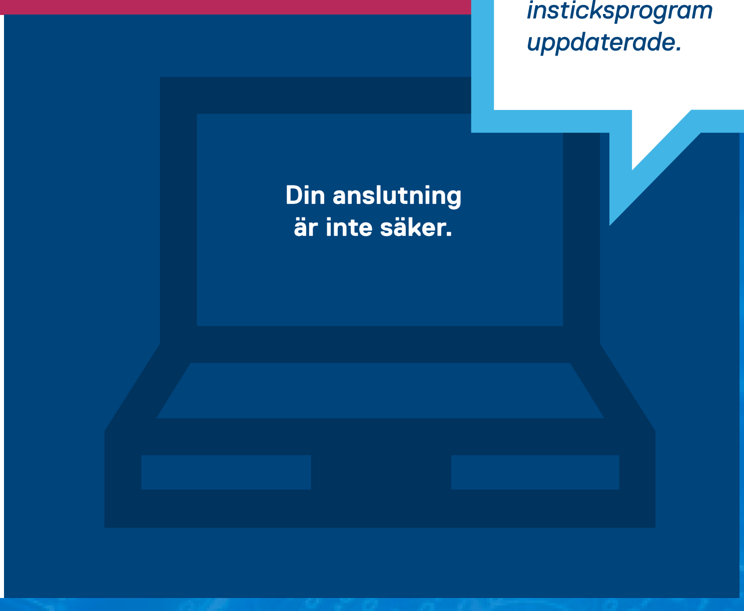
TIPS!
Håll webbläsare och insticksprogram uppdaterade.

Angripare med skadligt uppsåt får åtkomst till ditt system när du stöter på en osäker eller komprometterad webbplats.

Tecken att hålla utkik efter:

Nya filer eller nätverksanslutningar som du inte har lagt till dyker upp i systemet.

Oväntade förfrågningar om konfigurationsinformation.



Osäker maskinvara

TIPS!
Köp från auktoriserade säljare.

Hotaktörer bäddar in säkerhetsproblem direkt i maskinvara och tillbehör.

Tecken att hålla utkik efter:

Erbjudanden som är för bra för att vara sanna

Socialteknik

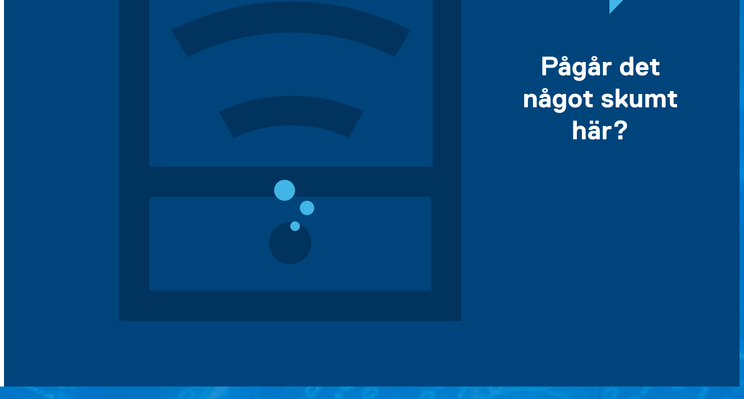
TIPS!
Myndighetsorgan (skatteverket o.s.v.) kontaktar dig via postverket först.

Bedragare manipulerar människor genom att låtsas vara polisen eller ett annat myndighetsorgan för att stjäla känsliga **personuppgifter eller ekonomisk information** (vilket kallas ”nätfiske”). Den skadliga koden skickas via länkar eller bilagor till e-postmeddelanden, direktmeddelanden och sms.

Tecken att hålla utkik efter:

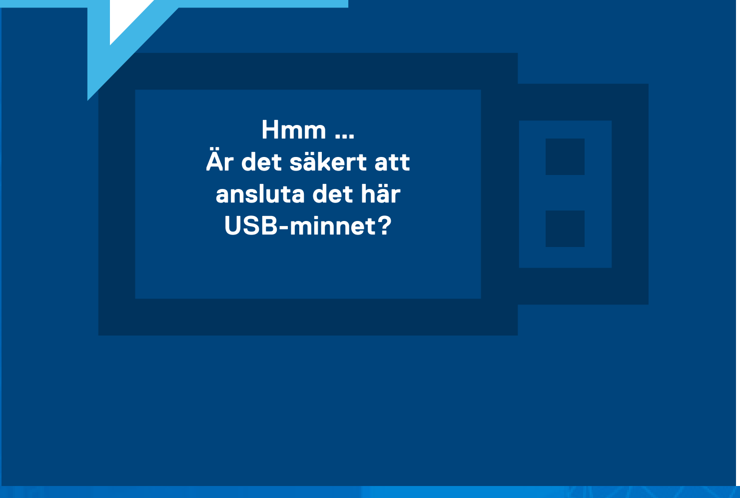
Oväntade e-postmeddelanden eller sms där avsändaren ber om personuppgifter, med öppna länkar eller bilagor.

Underlig avsändaradress, uttryck eller stavning.



USB-attack med skadligt program

TIPS!
Var försiktig med okända USB-minnen, även om du får dem från vänner.



Brottslingar använder borttagbara lagringsenheter, såsom USB-minnen, bärbara hårddiskar, smartphones, musikspelare, SD-kort och optisk media (CD, DVD, BluRay), för att infektera datorer och nätverk.

Tecken att hålla utkik efter:

Oväntad åtkomst till filer eller nyligen skapade filer på enheten.

Betrodda relationer

TIPS!
Använd starka och unika lösenord.

Hackare attackerar en betrodd tredje part, såsom en doktor, och använder hens rykte för att lura patienter.

Tecken att hålla utkik efter:

Ovanligt inloggningsbeteende.

Var cybersäker:

GÖR DETTA

Använd flerfaktorsautentisering och starka, unika lösenord för alla dina konton.

Alla enheter som är anslutna till internet kan attackeras. Håll programvaran uppdaterad.

Var skeptisk och på din vakt. Lär dig känna igen bedragares taktiker.

Säg ifrån. Rapportera attacker till IT-avdelningen och varna kollegor, släkt och vänner.

GÖR INTE DETTA

Var inte lat. Följ alla säkerhetsprotokoll konsekvent.

Klicka inte på länkar i oväntade e-postmeddelanden eller direktmeddelanden.

Ignorera inte varningar från webbläsaren, t.ex. ”Din anslutning är inte säker” eller ”Din anslutning är inte privat”.

TIPS!
Det finns mer information på Dell.com/Endpoint-Security

DELL Technologies

---

*Cybersecurity Ventures: 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics