



Säkerhet och Bedrägerier

Genom att vara medveten om de senaste trenderna och ta de nödvändiga försiktighetsåtgärderna kan du minska risken för att bli utsatt för ett cyberangrepp.

Länkar till tidigare presentationer

- [Undvik att bli lurad på nätet](#)
från Internetstiftelsen 27 september 2024
- [Tänk säkert och agera smart på nätet](#)
från Internetstiftelsen 11 oktober 2024 med sju olika videor.
- [Säkerhet på nätet](#)
Samlad information från Internetkunskap till dig som vill bli en mer medveten internetanvändare.

Olika typer av attacker

AI-genererade attacker: Artificiell intelligens används i allt större utsträckning för att skapa mer övertygande nätfiske-meddelanden och andra bedrägerier.

Deepfake-teknik: Förfälskade videor och ljudklipp, blir allt mer realistiska och kan användas för att lura människor att göra saker de annars inte skulle göra.

Ransomware-attacker: Angriparen krypterar data och kräver en lösensumma för att låsa upp den, fortsätter att vara ett stort problem.

Molnbaserade attacker: Allt eftersom fler organisationer flyttar sin data till molnet ökar också antalet attacker som riktar sig mot molntjänster.

IoT-attacker: Internet of Things-enheter, som smarta klockor och uppkopplade bilar, kan vara sårbara för attacker och användas för att komma åt andra nätverk.

För att skydda dig själv mot dessa hot är det viktigt att:

Ha starka lösenord:

Använd unika lösenord för varje konto och byt dem regelbundet. Använd "Lösenordshanterare"!

Vara försiktig med länkar och bilagor:

Klicka inte på länkar från okända avsändare.

Använda antivirusprogram:

Uppdatera antivirusprogram på din dator och andra enheter.

Uppdatera programvara:

Installera de senaste säkerhetsuppdateringarna för din programvara.

Vara medveten om de senaste bedrägerierna:

Håll dig informerad om de senaste bedrägerierna och hur du kan skydda dig.

Utbilda dig själv och andra:

Lär dig mer om cybersäkerhet och hur du kan skydda dig själv.

Tips! Lösenordshanterare

- **Välj en lösenordshanterare som passar dina behov och budget.**
Alla lösenordshanterare erbjuder olika funktioner och prisplaner, så det är viktigt att du väljer en som passar dig.
- **Se till att lösenordshanteraren har stark säkerhet.**
Detta inkluderar funktioner som kryptering, tvåfaktorsautentisering och en säker lösenordsgenerator.
- **Använd lösenordshanteraren regelbundet.**
För att få ut det mesta av din lösenordshanterare bör du använda den för att lagra alla dina lösenord och generera nya, starka lösenord.

Genom att använda en lösenordshanterare kan du skydda dina online-konton från hackare och göra ditt digitala liv säkrare.

Här är exempel på Lösenordshanterare

- 1Password - <https://1password.com/>
- Bitwarden - <https://bitwarden.com/>
- Dashlane - <https://www.dashlane.com/>
- NordPass - <https://nordpass.com/>
- LastPass - <https://www.lastpass.com/>
- Google - <https://passwords.google.com/>

