IT-SÄKERHET 2025: SÅ SKYDDAR DU DIG I EN DIGITAL VÄRLD

EN FÖRELÄSNING OM DIGITALA HOT OCH HUR VI SKYDDAR OSS

1. DET DIGITALA HOTLANDSKAPET

- VAD ÄR IT-SÄKERHET?
- ÖKANDE CYBERBROTT – STATISTIK FRÅN BRÅ
- EXEMPEL PÅ DAGENS HOT:
  - BLUFFMEJL OCH BLUFFSMS
  - AI-BEDRÄGERIER
  - DATAINTRÅNG

Vad är IT-säkerhet?

IT-säkerhet definieras som skyddet av digitala tillgångar, som system, nätverk och data, mot obehörig åtkomst, användning, avslöjande, ändring eller förstörelse.

Ökande cyberbrott – statistik från Brå

- **Anmälda bedrägerier:**
Totalt anmäldes 230 330 bedrägeribrott under 2024, vilket är en minskning med 3 % jämfört med 2023. Däremot är antalet anmälda bedrägerier 24 % högre än 2015.

- **Fakturabedrägerier:**
En ökning med 23 % under 2024, medan kortbedrägerier har minskat.

- **Social manipulation:**
Bedrägerier som sker genom social manipulation, exempelvis via telefon eller e-post, fortsätter att öka.

EXEMPEL PÅ BLUFFFAKTURA

Svensk Företagsregister AB
Organisationsnumo: 556999-1234

Avser
Registrering i Svenskt Företagsregister 2025

FAKTURA
Faktura nr: 24581
Belopp: 2 495 kr
Förfallodatum: 2025-11-05

Tack för din beställning av plats i vårt företagsregister! Ditt företag kommer nu att synas för tusentals kunder varje vecka.

Betala inom 10 dagar för att undvika påminnelseavgift.

Statistik från BRÅ

- **Ökad medvetenhet:**

Fler människor är medvetna om digitala bedrägerier och fler brott anmäls till polisen.

- **Nya metoder:**

Gärningsmännen utvecklar hela tiden nya metoder för att genomföra brott, exempelvis genom att utnyttja människors sociala sårbarheter.

- **Ökad digitalisering:**

Ju mer digitaliserat samhället är, desto fler potentiella måltavlor finns det för cyberbrott.

Ökande cyberbrott – statistik från Brå

- Vad du kan göra:

- **Var vaksam**

Var försiktig med e-post, sms och samtal som uppmanar till att lämna ut personlig information eller pengar.

- **Anmäl brott**

Om du blir utsatt för bedrägeri eller cyberbrott ska du anmäla det till polisen. Vår kommunpolis vill att vi anmäler även bedrägeriförsök.

CYBERBROTT IDAG – BEDRÄGERIER

- BANK-ID-BEDRÄGERIER, INVESTERINGSBLUFFAR, AI-RÖSTBEDRÄGERIER
- PHISHING, SMISHING, VISHING – FALSKA MEJL, SMS OCH SAMTAL

Bluffmejl (phishing)

Vanliga kännetecken

Tecken på bluffmejl	Exempel / förklaring
❗ Brådska och hot	”*Ditt konto stängs om du inte agerar NU*”
🖇 Misstänkt länk	Pekar på konstig webbadress t.ex. *seb-konto.ru; polisens.se*
📄 Bifogad fil	Ofta zip-, Word- eller pdf-fil som innehåller virus

Bluffmejl (phishing)

Vanliga kännetecken

Felaktig avsändaradress	t.ex. *support@swedb4nk.info*
Stavfel eller konstig svenska	Automatöversatt eller maskinöversatt text
Löfte om pengar	”Du har fått en återbäring /arv”
Vänlig men oväntad kontakt	”*Hej, kan du hjälpa mig köpa presentkort?*”

Bluffmejl (phishing)

Ett **bluffmejl** (även kallat **phishingmejl** eller *nätfiskemejl*) är ett falskt e-postmeddelande som är skickat i syfte att:

-  **Lura mottagaren att lämna ut känslig information** (t.ex. BankID, lösenord, kontonummer)

-  **Få mottagaren att betala pengar eller klicka på en länk**

-  **Sprida skadlig kod eller virus**

Hur ser ett bluffmejl ut?

Det är ofta utformat för att se ut som det kommer från en trovärdig källa, t.ex.:

- Din **bank** (SEB, Swedbank, Handelsbanken)
- **Skatteverket** (”Du har en återbäring att hämta”)
- **Postnord** / **DHL** (”Ditt paket är försenat, klicka här”)
- **Telia** / **Apple** / **Microsoft**

Exempl: Omedelbar åtgärd — obetald skatt

Hej kund,

Vi har inte mottagit din betalning för skatteåret 2024.
Ett krav har uttårdats på 5 320 SEK.

Klicka på länken nedan för att undvika vidare åtgärder:

Betala.nu http://skatteverket-payments.example.com

Vänligen uppdatera dina uppgifter omgående.

Mvh, Skatteverket
Ekonomiavdelning

Kort förklaring

•**Phishing** – Bedrägeri via **e-post** där angriparen försöker lura mottagaren att lämna ut lösenord, kortuppgifter eller klicka på en falsk länk.

•**Smishing** – Samma typ av bedrägeri, men sker via **SMS** (”SMS-phishing”). Meddelandet innehåller ofta en länk till en falsk webbplats.

•**Vishing** – Bedrägeri via **telefonsamtal** (”voice-phishing”). Bedragaren utger sig ofta för att vara från banken, polisen eller ett företag för att få offer att lämna ut känslig information.

AI-bedrägerier

Ett **AI-bedrägeri** är ett bedrägeri där bedragaren använder artificiell intelligens (AI) för att manipulera, imitera eller lura människor – ofta på ett mer övertygande och svårupptäckt sätt än traditionella metoder. Dessa bedrägerier har ökat kraftigt på senare år, i takt med att AI-tekniken blivit tillgänglig för allmänheten.

Vanliga typer av AI-bedrägerier

1. **Röstbedrägeri (deepfake voice)**

- AI används för att **imitera någons röst**, t.ex. en släkting, chef eller banktjänsteman.

Vanliga typer av AI-bedrägerier

1. Röstbedrägeri (deepfake voice)

- Offret får ett samtal där en välkänd röst ber om:
  - Pengar
  - En kod
  - Inloggning

- Exempel: ”Hej mormor, det är jag! Jag har problem, kan du Swisha mig?”

 En bluffröst kan skapas från bara 10 sekunders ljudinspelning!

AI-bedrägerier

AI-genererade mejl (phishing 2.0)

- Bluffmejl skrivs av AI så att de ser **mycket trovärdiga och korrekta ut.**
- Mejl kan anpassas till offret genom AI-analys av tidigare beteende.
- Exempel: AI skriver ett perfekt formulerat mejl från ”Skatteverket” som är omöjligt att skilja från ett äkta.

AI-bedrägerier

Falsk chatt eller kundtjänst

• Du tror att du chattar med en riktig bank eller support, men det är en AI som imiterar dem.

• Bedragare kan koppla in AI-chattbotar som lurar dig att:
    - Följa falska länkar
    - Göra betalningar

AI-bedrägerier

Romance fraud med AI

• AI-genererade bilder och text används i kärleksbedrägerier:

- Bilder på en "drömpartner"
- AI-chatt konverserar dygnet runt – romantiskt, trovärdigt, ihärdigt
- Offret skickar till slut pengar till en person som inte finns

Dataintrång

Du skyddar dig mot dataintrång genom att ha:

1. Starka och unika lösenord

2. Tvåfaktorsautentisering (t.ex. BankID eller kod via SMS)

3. Installera antivirus och brandväggar

4. Klicka inte på okända länkar eller bifogade filer

5. Använd uppdaterad programvara

2. MOBILTELEFONER – VANLIGA HOT OCH SKYDD

- SPIONAPPAR, QR-BEDRÄGERIER, FALSKA APPAR
- SKYDD: BIOMETRISK INLOGGNING, VPN, APPKONTROLL

2. DATORER & SURFPLATTOR – HOT OCH SKYDD

- HOT: KEYLOGGERS, FJÄRRSTYRNING, USB-ATTACKER
- SKYDD: ANTIVIRUS, SÄKERHETSUPPDATERINGAR, STARKA LÖSENORD

BankID-bedrägeri

Ett **BankID-bedrägeri** är ett **bedrägeri där en bedragare lurar en person att själv använda sitt BankID** – ofta i tron att det är en säker åtgärd – för att bedragaren ska kunna:

- Logga in på bankkonton
- Göra överföringar eller lån
- Komma åt Skatteverket, Pensionsmyndigheten eller liknande
- Utföra ID-kapning

Så går ett BankID-bedrägeri oftast till

📞 1. Bedragaren ringer upp

De utger sig för att vara från t.ex. banken, polisen, skatteverket eller MS-support:

💬 2. De skapar stress

De säger t.ex.:

- "Ditt konto är kapat – vi måste stoppa en överföring!"
- ”Vi ser en misstänkt inloggning från utlandet"
- ”Du har rätt till återbetalning/skatteåterbäring – vi behöver verifiera dig”

Så går ett BankID-bedrägeri oftast till

3. Du luras att identifiera dig

Du ombeds att:

- **Logga in med BankID**
- **Godkänna en säkerhetsåtgärd**
- **"Signera en återbetalning"** (som i själva verket är en kreditansökan eller överföring)

Så går ett BankID-bedrägeri oftast till

❗ **Men vad händer egentligen?**

När du identifierar dig eller signerar – **är det bedragarens åtgärd du godkänner.**

Det kan vara:

- Att ge dem tillgång till dina konton
- Att godkänna ett banklån i ditt namn
- Att ändra adress, telefonnummer eller spärrar

Så går ett BankID-bedrägeri oftast till

📈 **Hur vanligt är det?**
Enligt **Brå och MSB** ökar BankID-bedrägerier kraftigt, särskilt bland äldre.

2023 var det över **6 000 polisanmälningar** relaterade till BankID-bedrägerier
Ofta kopplat till telefonbedrägerier (s.k. vishing)

3. RANSOMWARE OCH SOCIAL MANIPULATION

- RANSOMWARE: KRYPTERING + LÖSENSUMMA
- SOCIAL ENGINEERING: TROVÄRDIGHET, STRESS, RÄDSLA

4. SKYDDSÅTGÄRDER – DIGITAL HYGIEN

- OLIKA LÖSENORD FÖR OLIKA TJÄNSTER
- TVÅFAKTORSAUTENTISERING (2FA)
- UPPDATERA MJUKVARA OCH ENHETER

SKYDDSÅTGÄRDER – BACKUP OCH VERKTYG

- AUTOMATISK BACKUP I MOLNET OCH OFFLINE
- REKOMMENDERADE VERKTYG:
  - LÖSENORDSHANTERARE: BITWARDEN, 1PASSWORD
  - VPN: PROTONVPN, MULLVAD
  - ANTIVIRUS: WINDOWS DEFENDER, MALWAREBYTES

5. FRAMTIDENS HOT: AI OCH IOT

- AI OCH DEEPFAKES: FALSKA RÖSTER OCH VIDEOR
- IOT: UPPKOPPLADE ENHETER SOM RISK – UPPDATERA ROUTRAR, BYT LÖSENORD

6. SAMMANFATTNING OCH SLUTSATSER

- DIN KUNSKAP ÄR DITT BÄSTA SKYDD
- TEKNIK HJÄLPER – MEN SUNT FÖRNUFT ÄR VIKTIGAST
- TACK FÖR IDAG!