

Minnesanteckningar från Föreläsningen om bedrägeri och IT-säkerhet. 20251106.

Arr: Kulturhuset Älta, Nacka kommun, Stöldskyddsföreningen och Polisen.

- **Brottsstatistiken** ökade år 2015 pga polisens omorganisation. Inte pga flyktigmottagandet. Ökat flyktigmottagande skedde även i Tyskland i samma grad som i Sverige och där ökade inte brotten. Källa: Jan Landström, Nacka kommuns säkerhetschef, kriminolog mm.
- **Nacka** ligger lågt i brottsstatistiken. Och **Älta** ligger ännu lägre. Bedrägerier ökar mest.
- Besök gärna **säkerhetskollen.se** och **ssf.nu** för tips eller ring tel: 0771-773 773. Det är stöldskyddsföreningen.
- **Nätfiske (phishing)**: Bluffmejl och falska webbsidor.
- **Telefonbedrägerier (vishing)**: Bedragare ringer och utger sig för att vara polis, bank mm.
- **SMS-bedrägerier (smishing)**: Falska SMS om vinster, paket etc. Anmäl bluff-SMS 7726.
- **Annons-och investeringsbedrägerier**: Falska annonser som lovar höga vinster.
- **Romansbedrägerier (catfishing)**: Falska profil med tjuvigt foto som vill få dig att sända pengar.
- **Id-kapning**: Någon använder dina personuppgifter för att beställa varor, sälja lägenhet/köpa hus, öppna konton eller skriva på avtal i ditt namn. Se hur du kan skydda dig längre ner. \*
- **Så skyddar du dig! De tre (3) L:n.**
  1. Lagg på telefonen om du känner dig osäker. Du behöver aldrig vara artig!
  2. Lämna aldrig ut personlig info till någon såsom kontokortsuppgifter.
  3. Logga aldrig in på Bank-id på uppmaning från någon. Om du loggar in kolla att rätt mottagare/företag står angiven!

#### **Kortbedrägerier – ett vanligt digitalt brott:**

Lås alltid ditt kort för internet- och utlandsköp.

Använd, skaffa gärna ett extrakort, separatkort som du handlar med. Ha lite pengar på kortet.

Försäkra dig om att företaget erbjuder säker betalning.

Lämna aldrig ut dina kortuppgifter till någon du inte känner, oavsett avsändare.

- **Spärra ditt kort** för internetköp och utlandsbetalningar.

#### **QR kods-bedrägeri**

QR koder som innehåller länkar till falska hemsidor eller skadlig kod.

Lurar av dig personliga uppgifter tex kontokortsinfo.

- **Qr-kodsbedrägerier (quishing)**: Leder till falska webbplatser. Förhandsgranska noga innan du läser av. Kolla webbadressen innan.

**Råd:**

Läs aldrig av QR koder på okända källor.

Förhandsgranska QR-koden om det går.

Lämna aldrig ut privat info.

Logga aldrig in på BankID om någon okänd uppmanar dig.

Gör en polisanmälan.

**Övriga tips och råd.**

- Om något verkar för bra att vara sant så är det nog inte sant. Jultomten finns inte.
- Var alltid kritisk om du får meddelande från någon okänd.
- Om du är osäker, så släng mejl, radera SMS direkt eller lägg på luren.
- Hitta.se (Adresslarm), Skatteverket (Adresslåset) och skaffa en digital brevlåda. Välj mellan KIVRA, BILLO eller MIN MYNDIGHETSPOST.
- Anmäl bluff-SMS till 7726
- För fler råd och tips eller tricks gå in på sakerhetskollen.se
- Om du har typ säkerhetskedja på din ytterdörr sätt på den om det ringer på din dörr. Ha den bara på när du öppnar dörren. Då är det lättare att utrymma bostaden snabbt.
  
- **Skatteverket har utmärkta sidor att läsa om: ID-kapning, Digital brevlåda, Om någon anmäler flytt till din bostad.**

Telefonnr: 112 Pågående brott. 114 14 Polisen, om du misstänker att någon försökt att lura dig eller utsatt dig för brott.

Alla uppgifter är hämtade från broschyrer och bilder som visades på Föreläsningen.

Vid datorn: Anette Ahston