Datafiske

Datafiske är ett ekonomiskt gynnande för anskaffande av information som t.ex. bankkoder, kreditkortsnummer eller personuppgifter. Personliga eller församlingsdata kan fås från falska e-postmeddelanden eller onlinetjänster.

Du kan få ett e-postmeddelande med en autentisk fråga för att säkerställa webbtjänstens funktionalitet som ber mottagaren att meddela användarnamn, lösenord eller övrig personlig information. Användaren kan också lockas av ett e-postmeddelande till en webbplats för att lämna ut information. Webbplatsen kan vara externt, till exempel en finansiell institutions sidor. I verkligheten är dessa webbplatser bluffwebbplatser som skapats av angriparen, där den angivnes data hamnar i angriparens händer.

De så kallade nigerianska brev lovar mycket pengar om du helt enkelt gör en "nominell" penning överföring till avsändarens konto, till exempel för att överföra eller beskatta pengar. Stora utlovade pengar är onödigt att vänta sig. Offren brukar kontaktas per e-post, ibland via fax eller post.

☒ Företag som sysslar med pålitlig affärsverksamhet, t. ex. banker, ber dig inte att skicka eller uppdatera information via e-post. Dessa meddelanden ska inte besvaras eller klickas på länkarna.

☒ Lita inte på innehållet i fältet avsändarinformation i e-postmeddelandet. Emailfältets avsändarinformation kan enkelt vara fejkade, t. ex.kundservice@dinegenbank.fi.

☒ Lita inte på att länkarna i din e-post eller webbplats kommer att leda till vart länkar visar.

☒ Det säkraste sättet att besöka webbplatsen för e-tjänster är att skriva självbetjäning

Webbsidans adress i webbläsarens adressfält, eller använd en snabblänk som du gör själv i webbläsaren (favoriter etc.).

☒ Kontrollera alltid innan du anger konfidentiell information om du är i rätt organisations

webbplats, och att webbplatsen har SSL-säkerhet. Online bank i adress fältet

En bankdomäns namn måste visas i adressen. Webbplatsen använder SSL-skyddet som

visas i webbläsaren stängs och adressen i adressfältet börjar med HTTPS-text.