Punainen Risti

Uppdaterad: 8.9.2025

ANVISNINGAR FÖR AVDELNINGARNA

Anvisningar om informationssäkerhet för frivilliga

Allmänna anvisningar

- Förvara personuppgifter utom syn-, hör- och räckhåll för utomstående.
- Tala inte om konfidentiella ärenden på offentliga platser.
- Använd spärrkod i mobila apparater och skärmskydd på bärbara datorer.
- Lås din bärbara dator när du lämnar (windows + L) arbetsstationen.
- Lämna inte dina apparater obevakade.
- Undvik öppna och oskyddade nätverk. Använd endast kända nätverk som är skyddade med lösenord.
- Använd starka lösenord för kontona och flerfaktorsautentisering.
- Välj applikationerna omsorgsfullt och håll dem uppdaterade.
- Starta om dina apparater varje vecka.
- Behandla konstiga e-postmeddelanden och telefonsamtal med sund misstänksamhet.

Starkt lösenord

Ett bra lösenord är långt (minst 15 tecken) och innehåller både stora och små bokstäver, siffror och specialtecken. Använd ett unikt lösenord i varje tjänst. Berätta aldrig ditt lösenord för någon.

Multifaktorautentisering (MFA)

Multifaktorautentisering, eller MFA, innebär att du vid inloggningen måste bekräfta den till exempel med en verifieringskod som skickas till telefonen. MFA förbättrar säkerheten avsevärt, för även om ditt lösenord skulle läcka ut eller hamna i fel händer kan angriparen inte logga in utan din autentiseringsmetod.

Använd därför MFA alltid när det är möjligt.

Acceptera MFA-begäran endast när du själv försöker logga in på tjänsten. Om du får en överraskande eller oväntad bekräftelsebegäran via telefonen ska du inte acceptera den, eftersom den kan vara ett tecken på att någon försöker komma åt ditt konto utan din tillåtelse.

Misstänkta meddelanden

Om du inte är säker på vem som skickat meddelandet eller innehållet i det, kontrollera saken till exempel genom att ringa avsändaren.

Om du får ett misstänkt meddelande ska du inte öppna bilagorna eller länkarna i meddelandet. OM du av misstag klickar på en länk i meddelandet som tar dig till inloggningswebbsida ska du inte skriva in ditt användarnamn och lösenord.

Byt ditt lösenord och kontakta FRK:s it-stöd itspr@rodakorset.fi **omedelbart** om du har klickat på en misstänkt länk eller angett dina inloggningsuppgifter på en misstänkt webbplats.

Kännetecken för att identifiera ett bluffmeddelande:

1. Avsändarens adress är misstänkt
   Adressen kan se riktig ut vid en snabb blick, men den skiljer sig något från den riktiga adressen (t.ex. m1crosoft.com jämfört med microsoft.com).
   Håll muspekaren över avsändarens adress för att se den verkliga avsändaren. Lita inte på enbart avsändarens namn, utan kontrollera även avsändarens e-postadress.

2. Akta dig för brådskande och hotfulla meddelanden
   Bluffmeddelanden försöker skapa en känsla av brådska: ”Ditt konto kommer att stängas”, ”Agera omedelbart”, ”Betalning krävs omedelbart”. Bedragare kan också utpressa och hota till exempel med att du förlorar anseende och egendom. Syftet med sådana meddelanden är att få dig att agera snabbt utan eftertanke.
   Förhasta dig inte, och fundera på om meddelandet låter logiskt och om du väntat dig ett sådant meddelande.

3. Grammatik- och stavfel
   Läs meddelandet noggrant. Bluffmeddelanden kan ofta innehålla en hel del stavfel, dåligt språk och översättningsfel. Felaktig grammatik kan vara ett tecken på ett bluffmeddelande som genererats av artificiell intelligens.

Kontrollera också meddelandets layout och underskrift. Saknas det en logotyp, kontaktuppgifter eller kanske en officiell underskrift i meddelandet? Äkta meddelanden har vanligtvis ett igenkännbart varumärke.

4. Kontrollera länken innan du klickar
   Texten i länken kan verka äkta, men i själva verket kan adressen ta dig till en bluffwebbplats. Kontrollera om länken är äkta genom att föra muspekaren över den och se vart den faktiskt tar dig. Klicka inte på länken om du inte är säker på att den är äkta.

5. Lämna aldrig ut ditt lösenord eller personlig information
   Tillförlitliga parter ber aldrig om ditt lösenord, dina bankuppgifter eller din personbeteckning via e-post. Ange dina inloggningsuppgifter endast på officiella inloggningssidor och använd multifaktorautentisering när det är möjligt.