

Information om IT sikkerhedshændelse.

Erhvervsskolerne Aars har desværre været udsat for et phishing angreb, hvor enkelte medarbejdere er blevet franarret adgangskode til deres mailboks. Tidligere var det nemmere at gennemskue falske beskeder og mails, fordi de for eksempel var skrevet på dårligt dansk, men nu er bagmændene mere professionelle, og de finder hele tiden nye metoder.

Resultatet er, at der i få timer har været uberettiget adgang til de pågældende medarbejderes mailboks.

Formålet har med stor sandsynlighed udelukkende været at kunne udsende spam.

IT-afdelingen lukkede adgangen til de konkrete mailbokse hurtigst muligt.

Mailadresser er blevet registreret/høstet, og nogle er brugt som modtagere spammail.

Hvad kan du gøre i tilfælde af phishing/spammail:

- Hvis du ved, det er phishing, så slet straks mailen eller beskeden.
- Hvis du er i tvivl, så tjek afsender adresse/nummer. Du kan eventuelt google det, og se om der kommer advarsler frem.
- Hvis du har en meddelelse med et link, så kan du normalt køre musen hen over linket uden at trykke på musen, og se om linket også linker til det, du tror, det gør.
- Husk, at de fleste virksomheder, som har adgangskoder og lignende, normalt aldrig vil kontakte dig med en neutral mail eller sms, hvis der opstår problemer.
- Kontakt virksomheden eller personen, der står som afsender, og hør, om de har sendt meddelelsen. Virksomheder vil gerne advares, hvis der er falske meddelelser i omløb med deres navn, og dine venner vil gerne vide, hvis deres mailkonto er blevet hacket. Kontakt dem aldrig via den meddelelse, der kan være falsk, men brug dine normale kontaktoplysninger på dem.
- Hvis skaden er sket, og du har givet de oplysninger, du blev bedt om, så spær straks den konto eller virksomhed, det vedrører. Hold øje med dine konti, og kontakt banken eller virksomheden, hvis der opstår uregelmæssigheder.
- Hvis du har klikket på et link, du ikke skulle, og straks opdager det, så kan du forsøge at minimere skaden ved straks at koble computeren af nettet. Kontakt en ekspert med henblik på at få rensset din computer.

Ved phishing hændelsen har der også været mulighed for brud på personers fortrolighed i forhold til indhold i mails.

Vi skal understrege, at vi **ikke** har set noget tegn på, at der er lækket oplysninger, og vi har naturligvis sikret de pågældende mailkonti efterfølgende.

I henhold til lovgivningen har vi anmeldt hændelsen til Datatilsynet og evt. berørte er kontaktet direkte.

Vi har en høj sikkerhed omkring personoplysninger, men nye angreb kan være svære at forudse og foregribe, selvom vi hele tiden justerer sikkerhedstiltag for at modvirke episoder som denne.

Vi undskylder meget den ulejlighed, dette måtte have forvoldt.