Incidentrapportringsprocess vid nätfiske

Nätfiskeattacker/phising attacks är idag den vanligaste metoden för en angripare att komma åt din/vår information och det sker i form av mejl, sms och telefonsamtal. Det är ett massutskick som syftar till att lura dig som användare att utge känslig information, till exempel inloggningsuppgifter och bankkontonummer. När avsändaren fått tag på informationen är tanken att den skall användas i olagligt syfte som att ta ut pengar från bankkonton utan innehavarens vetskap och tillåtelse eller att logga in på system för att utföra vidare attacker.

Huvudregel

Var alltid uppmärksam och ifrågasättande när du får mejl, sms eller ett telefonsamtal som vill att du ska utföra en aktiv handling. I en phishing-attack kan angriparen utge sig vara din chef, kollega, en myndighet, din bank etcetera - allt för att du skall tro att det är legitimt. Var alltid kritisk/ifrågasättande om de vill att du ska klicka på en länk, öppna en bilaga eller uppge någon information.

Vid mejl och sms

Rapportera in när du får misstänksamma mejl i din inkorg till IT-enheten genom att lägga ett ärende till helpdesk@ystad.se. Kontakta inte avsändaren genom att svara på mejlet eller att ringa upp personen med angivet nummer i mejlet, då det bekräftar att din adress är aktiv. Får man ett e-postmeddelande som är tveksamt skall man alltid verifiera med den person som står som avsändare. Var kritisk! Har du uppgett några inloggningsuppgifter, byt lösenord! Samma princip gäller vid sms, ring inte numret i sms:et och klicka inte på några länkar.

Vid en situation där du har klickat på en länk, öppnat en bilaga eller angett några uppgifter kontakta omedelbart IT-enheten via 0411–577001 och lägg ett ärende till helpdesk@ystad.se.

Vid telefonsamtal

- Logga aldrig in eller lämna ut dina uppgifter på uppmaning av någon annan.

Vid en incident eller misstanke av incident:

Identifiera och rapportera

- Misstänker du att du har blivit utsatt för nätfiske ska du **omedelbart rapportera** in det till IT-enheten genom att ringa dem på 0411–577001 och lägg ett ärende till helpdesk@ystad.se. Ge detaljerad information, skärmdumpar och annan relevant information som kan hjälpa dig och IT-enheten att hantera händelsen. Vidarebefordra inte mejlet till IT-enheten!

Försiktighetsåtgärder:

- Granska all mejl noggrant innan du klickar på en länk eller öppnar en bifogad fil. Ställ dig frågorna: Är meddelandet förväntat? Brukar avsändaren uttrycka sig på det här sättet?
- Undvik att klicka på länkar, sök i stället upp länken via betrodda källor.
- Var vaksam och öppna inte bilagor eller klicka på länkar i mejlet om du är osäker.
- Var extra försiktig om mejlet uppmanar dig till att agera snabbt, att verifiera dig och om avsändaren vill att du ska lämna ut andra typer av uppgifter.
- Är du osäker på avsändaren bör du verifiera den via andra kanaler än de som anges i mejlet. Om du inte kan verifiera avsändaren avstå då från att öppna/klicka på något. Kontakta IT-enheten i stället och låt dem hjälpa dig med ditt ärende.

Vidta åtgärder för att minimera skada

- Om du misstänker att dina inloggningsuppgifter har röjts, byt lösenord omedelbart genom att surfa till portal.ystad.se och ändra ditt lösenord. Använder du samma eller liknande lösenord på andra ställen – se till att byta där med.
- Vid misstanke om skadlig kod eller om datorn inte fungerar som vanligt kontakta IT-enheten. De hjälper till att genomsöka din dator för obehörig aktivitet och för skadlig kod.

Utbilda och informera varandra

- Har du råkat ut för nätfiske informera dina kollegor så de kan vara uppmärksamma att det cirkulerar mejl de bör vara vaksamma på. Vidarebefordra inte mejlet!
- Håll er uppdaterade om de senaste nätfisketrenderna via din organisation och genom omvärldsbevakning.

Säkra före det osäkra

Kontakta alltid IT-enheten om du är osäker på hur du ska agera vid en uppkommen IT-säkerhetsrelaterad händelse.

Kontaktuppgifter:

Mejl: helpdesk@ystad.se

Telefon: 0411–577001