Quick-guide til sikker håndtering af phishing

Hvad er phishing?

Phishing er et forsøg på at få fat i folks private informationer vha. forskellige metoder, fx via links eller vedhæftninger i mails eller sms'er.

Sådan spotter du et phishing-forsøg

- ***Du bliver bedt om at oplyse MitID og adgangskoder:*** Hverken AU, Nets, banker eller andre myndigheder vil sende en mail, hvor de beder dig om at oplyse adgangskoder, MitID mm.
- ***Du bliver bedt om at klikke på et link eller åbne vedhæftede filer:*** Vær varsom med at klikke på links og vedhæftninger i mails og sms'er. Gå i stedet igennem afsenderens officielle hjemmeside.
- ***Hold musen hen over links uden at trykke på linket:*** Så kan du se, hvor linket vil lede dig hen, inden du klikker. Her vil man ofte kunne se, at linket ser mærkeligt ud.
- ***Tegn på svindel i sproget:*** Falske mails og sms'er er ofte maskinoversatte. Se derfor efter usædvanlige formuleringer og stavefejl.
- ***Afsenderen:*** Hold musen hen over afsenderens navn for at se mailadressen. Er du i tvivl, om afsenderen er en svindler, kan du søge på nette og tjekke mailadressen eller kontakte virksomheden og bekræfte, at mailen er fra dem.
- ***Phishing- mailen er "forklædt" som intern mail:*** Svindlerne kan lave mailadresser, der til forveksling ligner AU-mailadresser. Vær opmærksom på små stavefejl i domænet fx @uniau.dk i stedet for @au.dk. Eller '@postnord.org' i stedet for '@postnord.dk'.
- ***Vent med at klikke og spørg evt. en kollega:*** Svindlere vil ofte få os til at handle i en fart, men hvis du uopfordret modtage en mail eller sms, er det en god idé at vente med at svare eller klikke, indtil du har god tid, eller du har talt med en kollega.

Sådan gør du, hvis du er faldet for phishing

- Det sker for flere, end du tror.
- *Du skal kontakte din lokale IT-support*, hvis uheldet er ude, og du er kommet til at klikke på et link, åbne en vedhæftet fil i en phishingmail eller har videregivet fortrolige oplysninger, som fx din adgangskode.

- Er du kommet til at videregive fortrolige oplysninger, skal du desuden hurtigst muligt ændre din adgangskode. Derudover bør du aktivere totrinsbekræftelse alle steder, du kan.
- Del gerne din oplevelse med dine kolleger. På den måde kan du være med til at advare andre og vi bliver alle sammen klogere.

Indrapportering af phishing-forsøg:

Microsoft indfanger størstedelen af indgående spam/phishing mails.

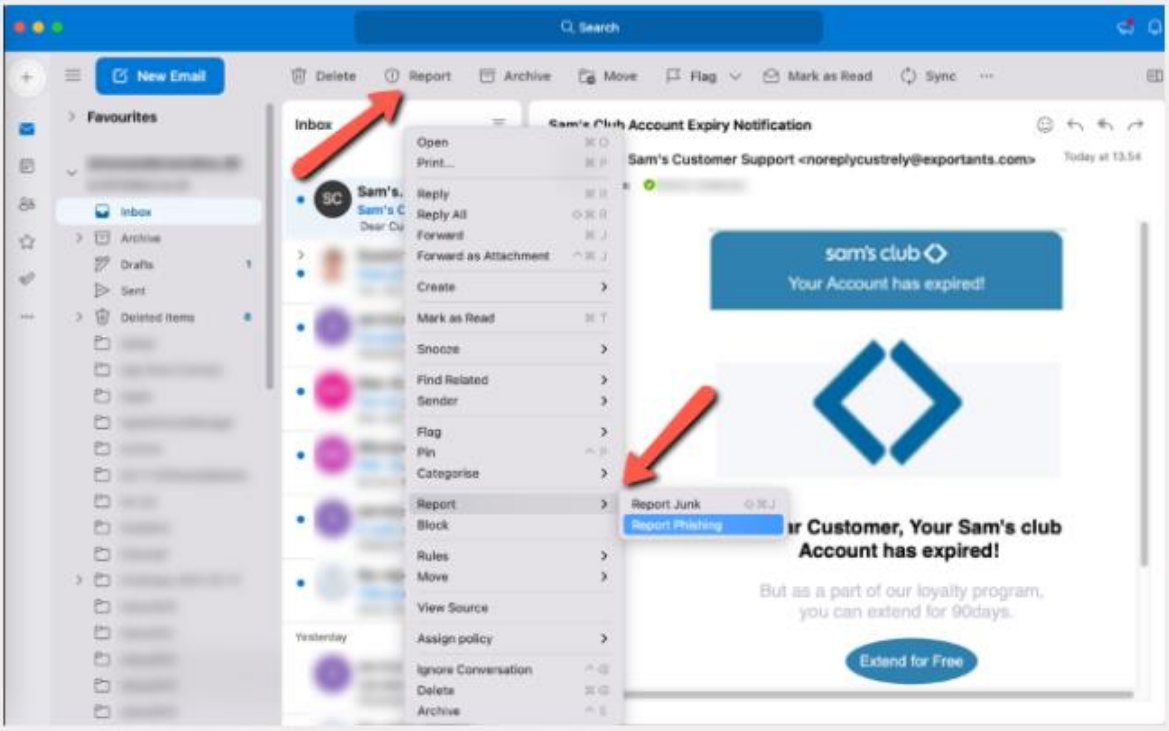
Hvis du alligevel skulle modtage en phishing mail, opfordres du til at indrapportere mailen for at sikre, at Microsoft hurtigst muligt kan lukke ned for phishing-mailen. Se nedenstående vejledninger.

Hvis du modtager en phishing sms, skal du kontakte din lokale IT-support.

Mac Computer

Hvis mailen er åbn, klik på Report -> Report Phishing

Man kan også højreklikke på mailen i listeoversigten og herfra vælge "Report as Phishing"

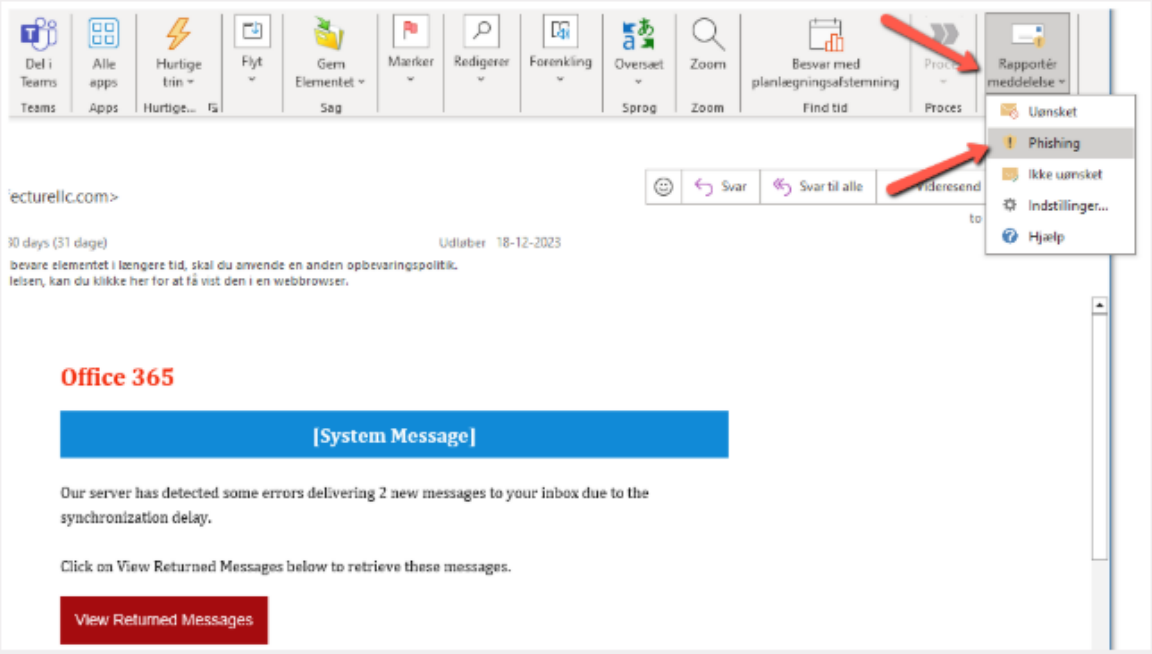


Windows PC

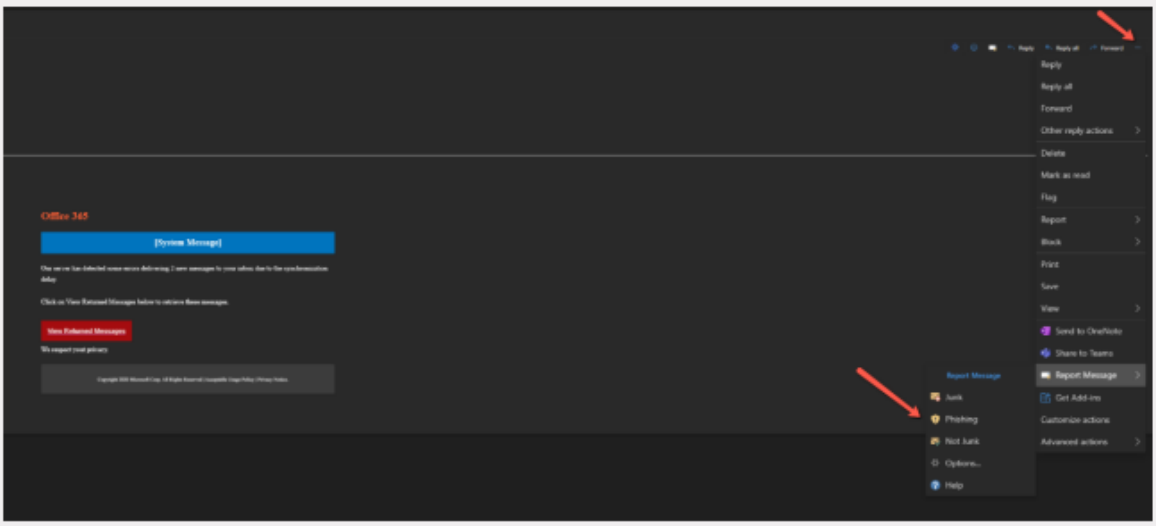
Skærmbillederne er lidt forskellige afhængig af, om du arbejder i outlook klienten eller i webmail, men fremgangsmåden er næsten den samme.

1. I øverste højre hjørne af den åbne mail klik på "Rapporter meddelelse"
2. Klik på "phishing" og klik efterfølgende på "rapporter meddelelse"
3. Mailen bliver nu registreret som phishing af Microsoft

Indrapportering af phishing i Outlook 365 (gammelt view)



Indrapportering af phishing i Outlook 365 (nyt view)



Indrapportering af phishing i Outlook 365 (webmail)

Hvor kan jeg læse mere om IT-sikkerhed?

Du kan læse mere om IT-sikkerhed her:

Regler for informationssikkerhed på Aarhus Universitet

Kontaktoplysninger til IT-support

Du kan kontakte IT support ved at oprette en sag via support.au.dk eller kontakt dem på mail (adm.it@au.dk) eller telefon (87150955).

Senest opdateret af HBS d. 28.11.24