

REAGÉR KUN PÅ SIKRE BESKEDER

Modtager du spam, falske mails og beskeder, så kan det være forsøg på phishing. Klik aldrig på links i mails, hvis du er i tvivl om afsenderens pålidelighed.

Beskeder og mails kan være falske og have til formål at lokke fortrolige oplysninger eller penge ud af dig. Det er ikke kun på mail, via telefonopkald eller SMS, men også på Facebook og andre sociale medier, at det forekommer.

Husk på, at ingen reelle virksomheder eller myndigheder anmoder om dine betalingskortoplysninger, dit NemID eller andre log-in-informationer via mail eller sms. Tjek altid afsenderens mailadresse ved tvivl – og undlad at svare hvis indholdet i beskeden eller afsenderen ser mistænkelig ud.

Stol på din kritiske sans

- Giv aldrig følsomme personoplysninger eller log-in-information via e-mail, sms eller telefonopkald
- Klik først på links, når du har tjekket om webadressen passer med afsenderen
- Tænk dig om, før du logger ind via et direkte link i en mail eller sms
- Tjek afsenderens mailadresse ved tvivl – og undlad at svare hvis indholdet i beskeden eller afsenderen ser mistænkelig ud

Er du i tvivl, om du har klikket på noget usikkert så kontakt altid IT straks

Modtager du spam eller phishing mails, skal du gøre følgende:

- Hvis du ved at det er spam/phishing, skal du videresende mailen til spam@randers.dk og derefter slette mailen fra din indbakke.
- Hvis du er i tvivl, så opret en support sag hos IT.

