SLIK AVSLØRER DU FALSKE E-POSTER PÅ 1-2-3

1 SJEKK AVSENDER OG E-POSTADRESSE

Legitime aktører sender ikke e-post fra adresser som slutter på @gmail.com eller mer suspekte adresser som eksempelet under. Noen svindlere kjøper også domener som ligner på legitime, som rmicrosoft.corn der 'm' er byttet ut med 'r' og 'n' tett sammen.

2 PRØVER E-POSTEN Å STRESSE DEG?

Falske e-poster inneholder et budskap om at noe haster. Hvis du ikke svarer på forespørselen med en gang, vil en pakke bli returnert, et abonnement stenges, og så videre.

Ved å spille på frykt og stress, håper svindlerne at du gjør noe overilt – og glemmer å tenke rasjonelt.

Fra: Microsoft KontoTeam rudmarks@hotmail.com
Til: Mea@microsoft.com
Dato: 4. des. 2018, 14:32

Kjære Microsoft-brukere,

Vi herved informerer deg om at vi vil slutte å behandle e-posten din fra databasen vår fordi din konto ikke er oppdatert på våre data. For å få disse meldingene, klikk på linken nedenfor for å bekrefte identiteten din

Klikk her for å bekrefte identiteten din

Vi beklager problemet.

Bilde: Microsoft community

3 IKKE KLIKK PÅ LENKER DU ER USIKKER PÅ

Selv om det står 'Trykk her for å logge inn på Mine Sider' i e-posten, kan svindlerne ha lagt inn en helt annen lenke som gjerne fører til en falsk nettside. På en datamaskin kan du få en liten indikasjon på hvor lenken faktisk fører ved å holde musepekeren over lenken. Da vil nettadressen lenken fører til dukke opp nederst til venstre i nettleseren. Virker den mistenkelig? Ikke trykk!

Er du usikker på om en lenke er legitim, kan du heller gå til den offisielle siden til den oppgitte avsenderen og se om du får samme informasjon der.

Svindlere blir stadig smartere og phishing stadig mer sofistikert.
Les mer om hvordan du kan avsløre falske e-poster her:

SIKKERHETS-MÅNEDEN
OKTOBER 2024

DigiNordland