SLIK AVSLØRAR DU FALSKE E-POSTAR PÅ 1-2-3

1 SJEKK AVSENDAR OG E-POSTADRESSE

Legitime aktørar sender ikkje e-post frå adresser som sluttar på @gmail.com eller meir snuskete adresser som dømet under. Nokre svindlarar kjøper òg domene som liknar på legitime, som microsoft.com der "m" er bytt ut med "r" og "n" tett saman.

2 PRØVER E-POSTEN Å STRESSA DEG?

Falske e-postar ber ein bodskap om at noko har bråhast. Svarar du ikkje på førespurnaden med ein einaste gong, vil ein pakke gå retur, eit abonnement bli steng og så vidare.

Ved å spela på frykt og stress, håpar svindlarane på at du gjer noko overilt – og gløymer å tenkja 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 IKKJE KLIKK PÅ LENKJER DU ER USIKKER PÅ

Sjølv om det står "Trykk her for logga inn på Mine Sider" i e-posten, kan svindlarane ha sett inn ein heilt anna lenkje som gjerne fører til ei falsk nettside. På ei datamaskin kan du her få ein liten indikasjon på kvar lenkja faktisk førar, ved å halda muspekeren over lenkja. Då vil nettadressa lenkja fører til dukka opp nedst til venstre i nettlesaren. Verkar den suspekt? Ikkje trykk!

Er du usikker på om ei lenkje er legetim kan du heller oppsøkja den offisielle sida til den oppgitte avsendaren og sjå om du får same informasjon der.

Svindlarar blir stadig smartare og phishing stadig meir sofistikert.
Lese meir om korleis du kan avsløre falske e-postar her:

SIKKERHEITS-MÅNADEN
OKTOBER 2024

DIGI VESTLAND