

# INFORMASIE-TEGNOLOGIE

## INFORMATION TECHNOLOGY

### HOE OM PHISHING-POGINGS TE FNUIK

Ons word dikwels deur personeel en studente gevra wat hulle kan doen om phishing-aanvalle te stop en watter sagteware hulle kan installeer om te voorkom dat hulle slagoffers daarvan word. In sommige gevalle het studente selfs versoek dat hulle rekenaars reggemaak moet word en sagteware installeer moet word om phishing-aanvalle te blok.

Ongelukkig is dit ? onmoontlike versoek. Net soos jy ? gewone verkoue nie kan voorkom nie, maar eerder ? spesifieke lewensstyl en voorkomende maatreëls kan toepas om die risiko vir besmetting te voorkom, geld dieselfde vir phishing-aanvalle. En net soos verkoues, gaan kubersekuriteitsrisiko's altyd daar wees en sal hulle aanpas en verander. Solank daar mense is wat oningelig of nalatig is, sal phishing-aanvalle voortduur.

Die beste manier om jou risiko te verminder is om alle agterdochtige phishing-pogings aan te meld op die [ICT Partner Portal](#) . (Meer volledige inligting aan die einde van hierdie artikel) Intussen is hier `n paar basiese reëls wat jou kan help om phishing uit te ken:

- **Gebruik logika**  
Moet nooit op skakels kliek, lêers aflaai of aanhangsels oopmaak in e-pos of sosiale media nie, selfs al lyk dit of dit van ? bekende, betroubare bron kom.
- **Oppas vir kort skakels**  
Kyk veral krities na kort skakels. Hou altyd die muis oor `n webskakel in ? e-pos (bekend as "hovering") om te kyk of jy na die regte webwerf herlei word.
- **Lyk die e-pos verdag?**  
Lees dit weer. Baie phishing e-posse is voor-die-hand-liggend en sal onoortuigende en algemeen verdagte inhoud bevat.
- **Wees versigtig vir dreigemente en dringende spertye**  
Dreigemente en dringendheid, veral komende van ? skynbaar egte maatskappye, gee gou die phishing-poging weg. Ignoreer die bangmaaktruuks en kontak eerder die maatskappy telefonies.
- **Navigeer eerder veilig met HTTPS**  
Gebruik altyd, waar moontlik `n veilige webwerf, aangedui deur https:// en `n "slot" ikoon in die blaaiër se adresstaaf.
- **Moet nooit publieke, onseker Wi-Fi vir banksake, aankope of invoer van persoonlike inligting gebruik nie – dit sluit Maties Wi-Fi in**  
Gerief behoort nooit meer belangrik as veiligheid te wees nie.

Wanneer jy ? phishing e-pos ontvang, rapporteer dit so gou as moontlik. Daarna kan jy dit dadelik uitvee.

Jy kan dit rapporteer op die IT se versoekaantekenstelsel, die [ICT Partner Portal](#).

- Gaan na die [ICT Partner Portal](#).
- Vul jou inligting in en heg die e-pos as ? aanhangsel aan. Jou versoek sal outomaties aangeteken word en die nodige maatreëls sal getref word deur ons stelseladministrateurs om die res van die kampus te beskerm.

[ARTIKEL DEUR DAVID WILES]

Posted in:Kuberstrieroof, Sekuriteit, Wenke | Tagged: Cyber Security, Kuberstrieroof, Report Phishing | With 0 comments