INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

HOW TO AVOID PHISHING SCAMS

We are often asked by staff and students what they can do to stop phishing scams, and what software they should install to prevent them from becoming victims. In some cases students have asked us to fix their computers and to install software to block phishing scams.

Of course that request is impossible to fulfil. Phishing scams are like the common cold. Just like you cannot prevent the common cold, you can only adopt a lifestyle, and take precautionary measures to reduce your risk of infection. They will always be there and will always adapt and change. As long as there are people who are uninformed or careless who fall for these scams, phishing attacks will continue.

The best way to reduce your risk is to report all suspected phishing scams on ICT Partner Portal. (Full details at the end of this post). Here are some basic rules to help you to identify phishing scams:

- ***Use common sense***
  Never click on links, download files or open attachments in email or social media, even if it appears to be from a known, trusted source.
- ***Watch out for shortened links***
  Pay particularly close attention to shortened links. Always place your mouse over a web link in an email (known as "hovering") to see if you're being sent to the right website.
- ***Does the email look suspicious?***
  Read it again. Many phishing emails are obvious and will have implausible and generally suspicious content.
- ***Be wary of threats and urgent deadlines***
  Threats and urgency, especially coming from what claims to be a legitimate company, are a giveaway sign of phishing. Ignore the scare tactics and rather contact the company via phone.
- ***Browse securely with HTTPS***
  Always, where possible, use a secure website, indicated by https:// and a security "lock" icon in the browser's address bar, to browse.
- ***Never use public, unsecured Wi-Fi, including Maties Wi-Fi, for banking, shopping or entering personal information online***
  Convenience should never be more important than safety.

If you do receive a phishing e-mail, please report it as soon as possible. Once you have reported the spam or phishing mail, you can delete it immediately.

You can report this on IT's request logging system, the ICT Partner Portal.

- *Go to the ICT Partner Portal.*
- *Fill in your information and add the email as an attachment. Your request will automatically be logged on the system and the appropriate measures will be taken by the system administrators to protect the rest of campus.*

[ARTICLE BY DAVID WILES]

Posted in:Phishing,Security,Tips | Tagged:Cyber Security,Phishing,Report Phishing | With 0 comments