NCG

Cyber Security Guidance

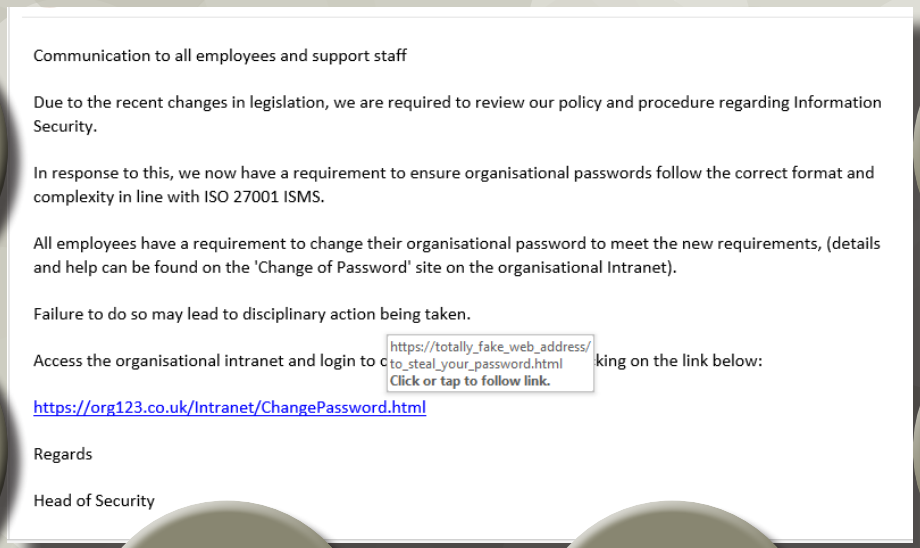
How to identify a suspected phishing e-mail

Phishing, pronounced "fishing," is a type of online identity theft that uses e-mail and fraudulent web sites that are designed to steal your personal data or information such as credit card numbers, passwords, account data, or other information. The general rule that should be applied is *'Do not supply any password, financial account or personal information via e-mail or the web, nor open any files attached to any e-mail unless you are expecting them and they are from a recognised, trusted source'*. The IT Department will never ask you to verify your details via email.

The image below is an example of a phishing email, please familiarise yourself with the awareness points situated around the email.

Emails may seem professional. The use of buzz words such as Legislation, Law, Policy and Procedure may be used to stress importance.

Look for poor spelling and grammar. As a rule, don't click on links withon an email uless you can confirm the integrity



Communication to all employees and support staff

Due to the recent changes in legislation, we are required to review our policy and procedure regarding Information Security.

In response to this, we now have a requirement to ensure organisational passwords follow the correct format and complexity in line with ISO 27001 ISMS.

All employees have a requirement to change their organisational password to meet the new requirements, (details and help can be found on the 'Change of Password' site on the organisational Intranet).

Failure to do so may lead to disciplinary action being taken.

Access the organisational intranet and login to c king on the link below:

https://totally_fake_web_address/to_steal_your_password.html
Click or tap to follow link.

https://org123.co.uk/Intranet/ChangePassword.html

Regards

Head of Security

Scaremongering tactics such as 'Disciplinary Action' may be used to try to force you to comply

Links within emails may look like the correct address, however may take you to a hoaxed and fake site to extract your details.

Hover over links contained within emails and ensure they point to the correct location.

Beware of realistic looking signature blocks. Details of individuals can be obtained from sites such as LinkedIn or Facebook

If you think you have received a phishing e-mail message, do not respond to it

If an e-mail looks suspicious, do not risk your personal information by responding to it. Do not reply to the email, nor click on any links in the email.

Approach links in e-mail messages with caution

Links in phishing e-mail messages often take you to phony sites that encourage you to transmit personal or financial information to con artists. Avoid clicking a link in an e-mail message unless you are sure of the real target address or URL.

Before you click a link, **make sure to read the target address**. If the e-mail message appears to come from your bank, but the target address is just a meaningless series of numbers, do not click the link.

Make sure that the spelling of words in the link matches what you expect. Fraudsters often use URLs with typos in them that are easy to overlook, such as "micosoft."

Don't trust the sender information in an e-mail message

Even if the e-mail message appears to come from a sender that you know and trust, use the same precautions that you would use with any other e-mail message.

Fraudsters can easily spoof the identity information in an e-mail message.

Type addresses directly into your browser or use your personal bookmarks

If you need to update your account information or change your password, visit the web site by using your personal book-mark or by typing the URL directly into your browser