

Subject: Totally plc. Increase in cyber-attacks – important communication from IM&T and Corporate Assurance

Phishing Emails Alert

Dear Colleague,

Increase in cyber-attacks during COVID-19 – how you can help to keep our systems safe!

We have recently received a number of targeted phishing emails, purporting to come from senior managers within Totally plc. It is likely that cyber-attacks will increase over Christmas, and so we ask you to be extra vigilant and ensure know what to look out for!

Some examples of the types of targeted emails may include:

- **Phishing**
In this type of attack, hackers impersonate a real company or sometimes an individual to obtain your login credentials. You may receive an email asking you to verify your account details with a link taking you to an imposter login screen that delivers your information directly to the attackers.
- **Spear Phishing**
Spear phishing is a more sophisticated phishing attack that includes customised information to make the attacker seem like a legitimate source. They may use your name and phone number and refer to Totally plc in the email to trick you into thinking they have a connection to you or the company. This is to make you more likely to click a link or attachment they've provided.
- **Whaling**
Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to ours, they look like normal emails from a high-level official of the company, typically the CEO or Finance Director, and ask you for sensitive information (including usernames and passwords).
- **Shared Document Phishing**
You may receive an email that appears to come from a file-sharing site like SharePoint alerting you that a document has been shared with you. The link provided in these emails will take you to a fake login page that mimics the real login page and will steal your account credentials.

If you do experience any kind of suspicious emails over the Christmas period – please email or call your line manager immediately. Please do not open any of the attachments in the email as this may cause further implications.

Thanks again for helping to keep our network and people safe from cyber threats. If you have any questions, please contact [REDACTED]

Many thanks,

[REDACTED]