CYBER CRIME

INTERNET SECURITY AWARENESS

THE INSURANCE CRIME BUREAU

5 WAYS TO SPOT FAKE EMAILS AND STAY SAFE

Unfortunately in today's world, Cyber Criminals are coming at organisations and individuals from all angles to try and trick us to part with our information. We all need to be **VIGILANT** in protecting ourselves online. There are numerous ways to detect fake emails or sites, phishing, etc. Here are some of the common ones.

No personalization or contact information

The email contains a generic salutation and/or lacks any contact information for the recipient to use if they have questions or require additional information.

Spelling and grammar errors

The email contains clear spelling or grammatical errors. Emails from legitimate companies are normally proof read extensively before being distributed.

Request personal information

The email requests that you follow a link to log into your account, or request personal information such as a credit card number, change pin or password.

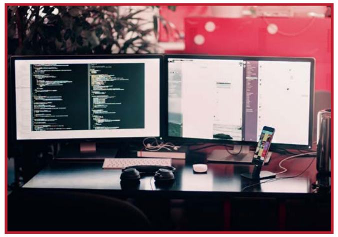
High urgency or threats

The email creates a high sense of urgency, or threatens consequences for inaction on the email is not received. This would usually happen late on a Friday afternoon.

REPLY URGENTLY OR ELSE!

Fake addresses or web links

The sender's displayed name and email address do not match the purported company the email represents, or the links send the recipient to other websites not associated with the purported company (E.g. www.company.nxt.com).



“INTELLIGENT PARTNERSHIPS”