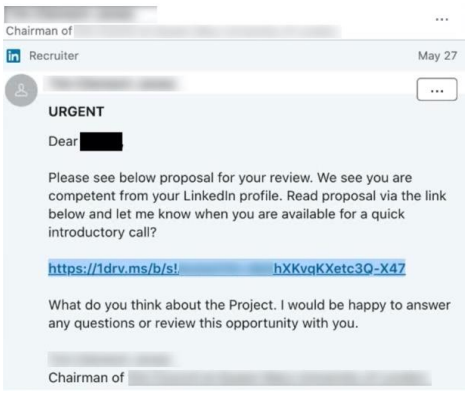
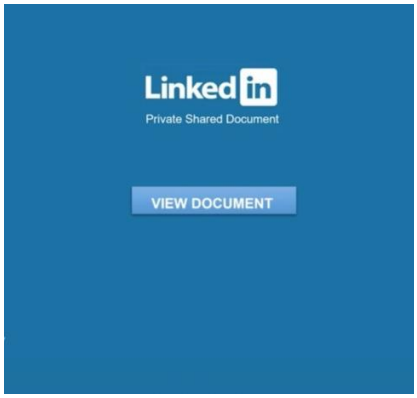
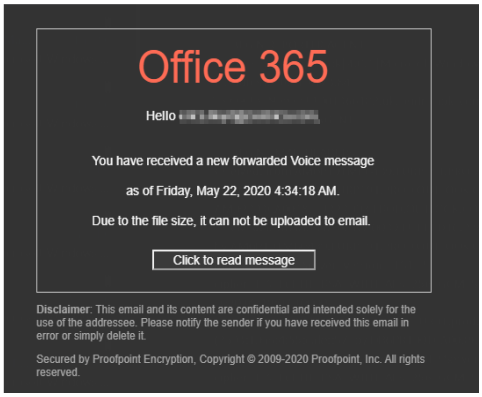
PSNI CYBER CRIME CENTRE

INFORMATION SHEET – 29/05/20

This information sheet has been compiled by the Police Service of Northern Ireland Cyber Crime Centre and is intended to raise awareness of current threats and available guidance. Advice and information is changing daily as we all navigate our way through the current COVID19 pandemic so please ensure you only take information from reputable sources.







Phishing examples

Thanks to Simon Whittaker at **Vertical Structure**, we are aware of this recent example of how a compromised LinkedIn account can be used to phish credentials. On clicking the One Drive link within the message, the recipient is met with a supposed LinkedIn document, which in turn diverts to a spoofed 365-login page.

Using the same method as seen in the Office 365 phishing example above shared by **Fujitsu**, the use of LinkedIn as a method of compromising an account is one many users may not be familiar with. A timely reminder of how a strong and separate email password not linked to Social Media accounts and **2FA** could help minimise the risk posed by an employee clicking that link.

NCSC support US National Security Agency advisory regarding the GRU (Russian military intelligence service)

Yesterday (28/05/2020) the NCSC supported the findings published by the **US National Security Agency** regarding "Russian Military cyber actors, publically known as Sandworm Team" and their exploitation of a vulnerability (CVE-2019-10149) in Exim mail transfer agent (MTA).

In late 2019, both the NSA and NCSC issued advice to mitigate against the risk posed by this vulnerability but as shown by our recent experiences with **VPN** and **Firewall** exploits, organisations can remain vulnerable to known exploits for some time after a patch is issued if the correct advice is not followed

Action Fraud update (May 29th 2020)

2,057 victims have lost a total of over £4.6 million to coronavirus related scams.

Locally, phishing and the exploitation of compromised email accounts continues to provide criminals the opportunity to divert incoming or outgoing invoices risking the loss of funds at a time when for many, finances are tight.

NCSC Suspicious Email Advice

Suspicious emails can be reported to the **NCSC Suspicious Email Reporting Service** - report@phishing.gov.uk

Useful websites
www.actionfraud.police.uk
www.ncsc.gov.uk/cyberaware
www.haveibeenpwned.com

Social Media
@PSNIBelfast
@cyberawaregov
@ncsc