PSNI CYBER CRIME CENTRE

INFORMATION SHEET – 07/05/20

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.

The latest **NCSC Weekly Threat Report** once again highlights the vulnerability posed to organisations using unpatched Sophos XG Firewalls. Unpatched vulnerabilities are a favoured attack method used by cyber criminals and we would encourage organisations to ask the questions do we use this? **and is it patched?**

NCSC Suspicious Email Reporting Service (SERS)

The latest update from the NCSC shows in its first week, the new SERS received over 25,000 reports leading to some 395 phishing sites targeting individuals and businesses being taken down!

Help support SERS be sharing details with staff.

Local news

On World Password Day, the NI Cyber Security Centre are asking users to consider taking a password pledge to secure online accounts and put an end to weak passwords.

For more info check out: **NICSC** and @NICYBERSC

Keep up to date

Whether it is to see recent phishing examples or keep up to date with the latest attack methods and IOC's (Indicators of Compromise), we would encourage organisations to look at the **NCSC CiSP** (Cyber Security Information Sharing Partnership). Alongside sector specific interest groups and updates from the NCSC, the CiSP has a regional Northern Ireland group where you can share experiences or questions securely and confidentially.

For more info, email **Cyber Protect**

Cyber Warning issued for key healthcare organisations in the UK and USA

Together with the US Cyber Security & Infrastructure Agency (CISA), the National Cyber Security Centre (NCSC) have issued an **advisory** advising staff in key healthcare and medical research organisations 'to change any passwords that could be reasonably guessed to one created with **three random words** and implement **two factor authentication** to reduce the threat of compromises'.

The advisory outlines how both agencies have identified targeting of national and international healthcare bodies, pharmaceutical companies, research organisations and local government with 'password spraying' a specifically referenced attack method.

As we have commented on before, incidents we see, from ransomware to email compromises frequently result from the use of poor passwords combined with a lack of 2FA or other readily available tool such as blocking unknown devices or IP addresses.

Alongside advice from **CyberAware** **and the NCSC e-learning package for staff**, why not check out the top 100,000 passwords seen by **HaveIBeenPwned**

NCSC Suspicious Email Reporting Service – forward suspicious emails to report@phishing.gov.uk
Did you know you can report spam sms on your phone to 7726 (SPAM)

Useful websites
www.actionfraud.police.uk
www.ncsc.gov.uk/cyberaware
www.nicybersecuritycentre.gov.uk

Social Media
@PSNIBelfast
@cyberawaregov
@ncsc