PSNI CYBER CRIME CENTRE

INFORMATION SHEET – 30/06/20

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.

Social Media Day

On what is **#socialmediaday** it is perhaps worth reflecting on the impact a compromised social media account could have on an account user be that your child, colleague or yourself.

Whether it results in using your photos or emailing contacts in your name for money, 2 common features in reports we see are it can be **incredibly difficult** to recover access to your account and if the 2FA offered by the service had been in place, the compromise would in most instances, not have taken place.

For a guide on how on set up 2FA on your accounts check out **https://www.telesign.com/turnon2fa**

Web Server Vulnerability

For those managing their own web server or doing so on behalf of a client, a recent **advisory** from the Australian Cyber Security Centre highlights a vulnerability in **Telerik UI** which can provide malicious actors server access and the ability to upload malicious files (CVE-2019-18935). Attackers have been testing and exploiting this patchable vulnerability and to date we have spoken with one local organisation identified as being at risk.

Suspicious Email Reporting Service

Those following our information sheets may recall that alongside Cyber Aware, we announced the launch of the NCSC Suspicious Email Reporting Service (SERS) back in April this year. Having been available for just 2 months, this innovative service has now received **one million reports** leading to 10,000 online scams being blocked or taken down.

Of note, more than half of the 10,000 online links reported to date relates to cryptocurrency investment scams, a fraud type which is being increasingly being seen across the UK. Whether it is the promise of low risk / high returns or the use of fake celebrity endorsements, this type of fraud can involve fake social media profiles and professional looking websites with one recent report to the Cyber Crime Centre involving the spoofing of a genuine NI company. **NCSC SERS UPDATE**

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

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

Social Media
@PSNIBelfast
@cyberawaregov
@ncsc