CYBERCRIME NEWS

ISSUE 10 • JULY 2024

ROBUST CYBER SECURITY

WHEN DID YOU LAST CHANGE YOUR PASSWORD?

IN TODAY'S DIGITAL LANDSCAPE, SAFEGUARDING PERSONAL AND BUSINESS DATA IS PARAMOUNT.

A large number of people use the same password for all of their accounts and personal log ins. For individuals, strong cyber security practices include using complex, unique passwords for each account and changing them regularly.

However, utilizing a reputable password manager and enabling multi-factor authentication (MFA) adds additional layers of protection.

Keeping software and operating systems updated is vital to close security gaps.

We have mentioned in previous newsletters that being vigilant with emails and links to avoid phishing scams is important but deploying reliable antivirus and anti-malware programs to detect and mitigate threats, are also critical steps.

TOP TIPS FOR PASSWORDS

THREE UNIQUE WORDS

CHANGE THE PASSWORD REGULARLY (EVERY 3 MONTHS)

FOR BUSINESSES, A ROBUST CYBER SECURITY STRATEGY IS ESSENTIAL

1 This starts with comprehensive employee training to recognise phishing attempts and understand the importance of data protection.

2 Implementing stringent access controls ensures only authorised personnel access sensitive information.

3 Regularly backing up data and storing it securely offsite can mitigate the impact of ransomware attacks.

4 Advanced firewalls and intrusion detection systems help prevent unauthorised access. Additionally, conducting regular security audits and penetration testing is critical to identifying and addressing vulnerabilities.

5 Recent events underscore the importance of these measures, you may well have been affected. Last week, a faulty software update that caused the global IT outage likely skipped checks before being deployed, experts have

said - as a warning was issued about malicious websites offering to fix devices.

6 An estimated 8.5 million Microsoft Windows PCs devices were affected worldwide by the update from cybersecurity firm CrowdStrike, causing delays for airports, broadcasters, hospitals and businesses. This incident emphasises the need for vigilant monitoring, timely updates, and proactive security measures even with trusted platforms.

7 Fixes are now available to resolve the issues, and affected organisations should refer to the relevant vendor guidance and take the necessary action.

8 Installing security updates is still an essential security practice and organisations should continue to install them when they are available. Organisations should also continue to use antivirus products as normal.

INCREASE IN PHISHING

NOTE THAT AN INCREASE IN PHISHING REFERENCING THIS OUTAGE HAS ALREADY BEEN OBSERVED SINCE, AS OPPORTUNISTIC MALICIOUS ACTORS SEEK TO TAKE ADVANTAGE OF THE SITUATION. THIS MAY BE AIMED AT BOTH ORGANISATIONS AND INDIVIDUALS.

Organisations should review NCSC guidance to make sure that multi-layer phishing mitigations are in place, while individuals should be alert to suspicious emails or messages on this topic and know what to look for.

Advice can be found on the Dorset Police Cyber Crime page of the website, don't forget there is a free tool funded by the Home Office that helps your business or organisation monitor and report the suspicious cyber activity it faces - Police CyberAlarm.

Police CyberAlarm monitors inbound traffic on your organisation's firewall. It can help you (and police) spot a possible attack in progress, or the signs that one may be being prepared for. Since launched it has identified over a billion suspicious events resulting in reports and advice being given to members, enabling them to take action to prevent a successful attack.

Staying informed about the latest cyber threats and evolving security practices is essential for both individuals and businesses. By implementing robust security measures and remaining vigilant, the risk of cyber attacks can be significantly reduced, ensuring a safer digital environment.

REPORTING CYBER CRIME

If you fall victim to fraud or cyber crime, you can report this to Action Fraud by visiting www.actionfraud.police.uk or by calling 0300 123 2040.

If you have received an email that you're not sure about, you can report this to the **National Cyber Security Centres Suspicious Email Reporting Service (SERS)**. Simply forward the email to **report@phishing.gov.uk**.

The SERS automatically analyses suspicious emails and, if it considers it to be malicious, can take steps to have email accounts and associated websites closed down, meaning each report can really make a difference.

DORSET POLICE

Dorset Police
Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

E cybercrimeprevention@dorset.pnn.police.uk
www.dorset.police.uk

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

Office of the Dorset Police & Crime Commissioner
Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

T 01202 229084
E pcc@dorset.pnn.police.uk
www.dorset.pcc.police.uk