ISSUE 4, 22 JUNE 2020
WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK

WM ROCU
Cyber Crime Sentinel

This newsletter has been collated by West Midlands Regional Cyber Crime Unit and is intended for wider distribution within the West Midlands Region to raise awareness among businesses and members of the public.



IN THE NEWS

Shopped with Claire's online? Hackers may have stolen your card details. Any customers who made purchases on Claire's website between April 30th and June 13th, should contact their card company and monitor statements for fraudulent purchases. https://news.sky.com/story/shopped-with-claires-online-hackers-may-have-stolen-your-card-details-12007303

Cycling equipment shop Wiggle were targeted in this type of attack and a small number of customer details were acquired. In response, Wiggle have taken steps to identify the compromised accounts and contact individual impacted. All accounts will now require the re-entry of card details for the next purchase. Wiggle customers are strongly advised, to change login passwords and check any cards previously used to make purchases.

Action Fraud has received reports from 2,378 victims of Coronavirus-related scams, with the total losses reaching over £7 million.
https://www.actionfraud.police.uk/campaign/covid-19-guidance-and-advice

Spies Can Eavesdrop by Watching a Light Bulb's Vibrations
https://www.wired.com/story/lamphone-light-bulb-vibration-spying/

Northampton-based cosmetics giant Avon is KO'd by worldwide cyber-attack
https://www.northamptonchron.co.uk/business/northampton-based-cosmetics-giant-avon-kod-worldwide-cyber-attack-2884686



AVOID SCORING A CYBER OWN GOAL WHEN STREAMING PREMIER LEAGUE'S RETURN

FOOTBALL fans have been warned of cyber threats when they swap their tickets for TV subscriptions – and been advised how to watch behind-closed-doors games as safely as possible.

The National Cyber Security Centre (NCSC) has shone a light on online criminals who could hack into accounts by guessing passwords that are obvious or have been compromised in the past. In a previous article, the NCSC revealed that almost 700,000 accounts have been compromised through hackers guessing a device's passwords as 'liverpool', 'chelsea' or 'arsenal'.

As well as illegally watching the game the victim has paid for, the hackers could make unauthorised purchases on the platform or look to find personal information that could be used for further scams – including targeting them with scam emails or phone calls.

For more information on this visit the NCSC website https://www.ncsc.gov.uk/news/football-fans-avoid-cyber-own-goal

SECURE YOUR VIEWING EXPERIENCE BY:

REFRESHING ACCOUNTS: It's a great time for fans to consider resetting their password. We're increasingly seeing hackers use credentials stolen in past security incidents to hijack streaming accounts using the same compromised details. If you're using the same password for your sports streaming accounts that you've used multiple times in the past – it's time for a reset.

SETTING A STRONG PASSWORD: We recommend using a password that's separate to your email password and made up of three random words. You can then save this strong password in the browser so you don't have to worry about remembering it.

Updating streaming apps: Cyber criminals exploit weaknesses in apps to access your sensitive personal data. Providers regularly issue patches to these exploits in updates – you're vulnerable without them so we urge every fan to make sure their streaming apps are updated. To make it simple going forward, we recommend turning on automatic updates



National Cyber Security Centre

Using passwords

To protect your devices & data

Passwords are an effective way to control access to your data, the devices you store it on, and the online services you use.This page contains tips about how to create strong passwords, how to look after them, and what to do if you think they've been stolen. For more information, please refer to **www.cyberaware.gov.uk** .



Criminals will use the most common passwords to try and access your accounts, or use information from your social media profiles to guess them. If successful, they will use this **same password** to try and access your **other accounts**.

Criminals also try and trick people into revealing their passwords by creating fake 'phishing' emails that **link to dodgy websites**, or by using **persuasive techniques** through social media.

Even if you look after your passwords, they can still be stolen if an organisation containing your details suffers a **data breach**. Criminals will use these stolen customer details (such as user names and passwords) to try and access other systems.

© Crown Copyright 2020

Create strong passwords



Create a strong and memorable password for your email account (and other important accounts).

Avoid using predictable passwords (such as **dates, family** and **pet names**). Avoid the most common passwords that criminals can easily guess (like 'passw0rd').

Don't re-use the same password across important accounts. If one of your passwords is stolen, you don't want the criminal to also get access to (for example) your banking account.

To create a **memorable password** that's also hard for someone else to guess, you can **combine three random words** to create a single password (for example *cupfishbiro*).

Look after your passwords



If you store your passwords somewhere safe, you won't have to remember them. This allows you to use unique, strong passwords for all your important accounts.

You can write your password down to remember it, but **keep it somewhere safe**, out of sight, and (most importantly) **away from your computer**.

Most web browsers will offer to store your online passwords. **It's safe to do this.** Browsers will also detect 'dodgy' websites that phishing emails try and trick you into visiting.

You can also use a standalone **password manager** app to help you create and store strong passwords.

Use 2FA to protect your account



Many companies allow you to set up two-factor authentication (also known as 2FA) on your accounts. It's called 2FA because it involves signing into your account using **two passwords or codes;** one that you know, and the other usually sent to your phone.

The most common form of 2FA is when a code is sent to your smartphone that you must enter in order to proceed. You should **set up 2FA for important websites** like banking and email.

Even if a criminal knows your passwords, they will struggle to access any accounts that you've protected by turning on 2FA.

TURN IT ON

The website **www.telesign.com/turnon2fa/** contains up-to-date instructions on how to set up 2FA across popular online services such as Gmail, Facebook, Twitter, LinkedIn, Outlook and Instagram.

What to do if your password is stolen?



If you suspect your password has been stolen, you should change it as soon as possible.

If you have used the same password on any other accounts, change these as well.

You can use the website **www.haveibeenpwned.com** to check if your information has ever been made public in a major data breach.

Dealing with Suspicious E-mails, Phone Calls and Text Messages

Recently, the NCSC have updated guidance on **"Dealing with suspicious emails, phone calls and text messages."** In the guidance, the NCSC discuss how to spot the most obvious signs of a scam, and what to do if you've already responded. They highlight a newer feature allowing suspicious text messages to be forwarded to 7726. This free-of-charge short code enables your provider to investigate the origin of the text and take action, if found to be malicious.

Find out more: https://www.ncsc.gov.uk/guidance/suspicious-email-actions

TECH TALK

NCSC Weekly Threat Report Topics

- New HMRC text message phishing scam targets self-employed
- IT services firm hit by Maze ransomware attack
- APTs continue to exploit vulnerabilities in several VPN products used worldwide

https://www.ncsc.gov.uk/report/weekly-threat-report-12th-june-2020

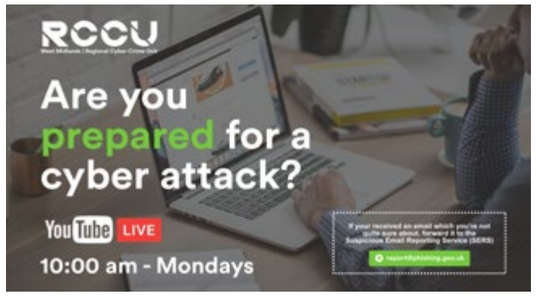
Vulnerabilities in D-Link router raises concerns over remote worker IT security
https://www.scmagazineuk.com/vulnerabilities-d-link-router-raises-concerns-remote-worker-security/article/1686501

Snake Ransomware Slithering Across Connected Networks
https://cyware.com/news/snake-ransomware-slithering-across-connected-networks-a6fce96b

Abnormal Attack Stories: COVID-19 Relief Phishing Through Dropbox Transfer
https://abnormalsecurity.com/blog/abnormal-attack-stories-covid-19-relief-phishing-through-dropbox-transfer/

BE CYBER AWARE

Although physical events have been rearranged for later dates, we've been providing inputs through video conferencing/remotely. We have done this internally for organisations, as well as for public business groups. If you would like an input for your own organisation or group, please get in touch.



ARE YOU PREPARED FOR A CYBER ATTACK?

On Mondays at 10am we will be hosting 'Are you prepared for a cyber attack?' presentations via YouTube Live available here:

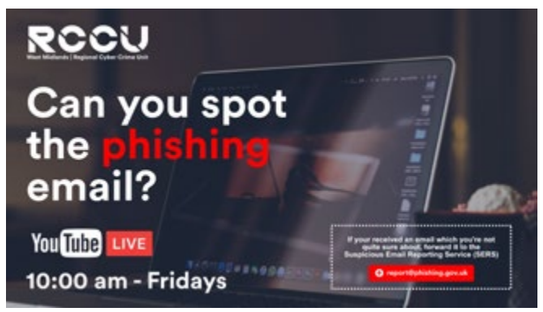
https://www.youtube.com/watch?v=__xyxqp2cqk



CYBER SECURITY LIVE Q&A

You will be able to join us at Sli.do every Wednesday to ask us questions and advice about cyber security and how to stay safe online. All the sessions will be held on sli.do, where you will also be able to see previous Q&As.

https://app.sli.do/event/jvodjdcu/



CAN YOU SPOT THE PHISHING EMAIL?

On Fridays at 10am we will be hosting 'Can you spot the Phishing Email?' presentations via YouTube Live available here: https://youtu.be/NuEbmZw7-5A



SIMPLE TIPS TO PROTECT YOUR BUSINESS FROM CYBERCRIME

Wed, 8 July 2020, 09:30 – 11:00

available here: https://www.fsb.org.uk/event-calendar/simple-top-tips-to-protect-your-business-from-on-line-fraud-cybercrime-attacks.html?aff=Twitter



CYBER THREAT WEEKLY

Our lives are relying on technology more every day. Join us each Monday for your bitesize cybersecurity podcast. In this increasingly technical world we deliver non-technical cyber news, and identify the current threats we're facing.

https://cyberthreatweekly.buzzsprout.com/

WM ROCU REGIONAL CYBER CRIME UNIT