ISSUE 4, 26 JUNE 2020
WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK
WWW.WMCYBER.ORG

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

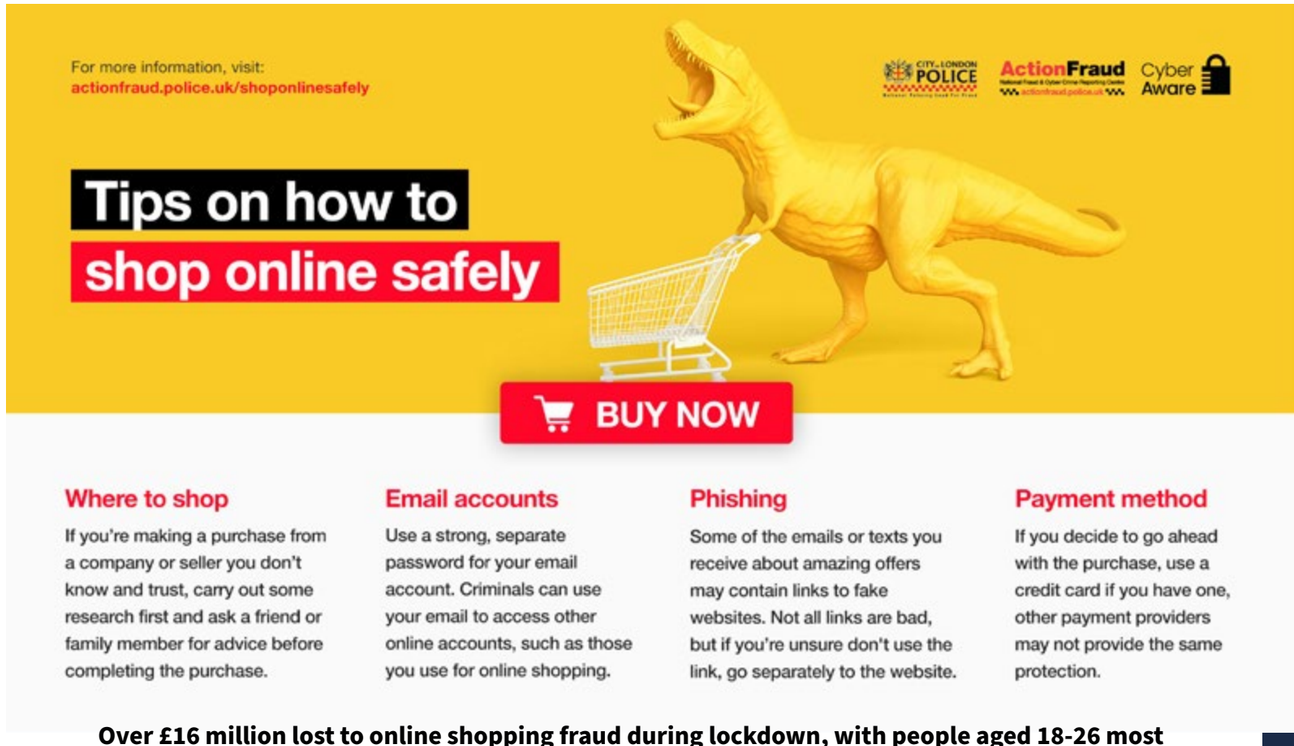
New Zealand seizes £72m of assets from alleged Russian cyber criminal
Police have seized assets worth NZ$140 million linked to a man suspected of laundering billions of dollars in digital currency. For more information, visit https://www.telegraph.co.uk/news/2020/06/23/new-zealand-seizes-72m-assets-alleged-russian-cyber-criminal/

Coronavirus: Scottish public sector bosses targeted by cyber criminals during lockdown
https://www.pressandjournal.co.uk/fp/news/politics/scottish-politics/2279153/coronavirus-scottish-public-sector-bosses-targeted-by-cyber-criminals-during-lockdown/

MMO Game Stalker Online Hacked - 1.2 Million User Records Put for Sale on Hacker Forums
https://cybernews.com/security/popular-mmo-game-stalker-online-hacked-1-2-million-user-records-put-for-sale-on-hacker-forums/

Phishing attack impersonates LinkedIn notification
It has come to our attention hat threat actors are impersonating a LinkedIn email template in an attempt to steal user login credentials. The email pretends to be a notification from LinkedIn relating to a potential business partnership. The payload links in the emails to a compromised website, but the phishing page looks similar to the login page for LinkedIn. For LinkedIn Security Advice visit: https://safety.linkedin.com/identifying-abuse

Cyber Threat Weekly: Holiday Fraud Episode
Episode: https://www.buzzsprout.com/1135268/4299596-holiday-fraud.mp3?blob_id=16734116
Its summer but unfortunately holidays have been limited. Due to current events large numbers have had holidays cancelled. This unfortunately is something the cyber criminal is taking advantage of. After listening to this podcast please visit Action Fraud and the National Cyber Security Centre for more guidance.



Over £16 million lost to online shopping fraud during lockdown, with people aged 18-26 most at risk
https://www.actionfraud.police.uk/alert/over-16-million-lost-to-online-shopping-fraud-during-lockdown-with-people-aged-18-26-most-at-risk

Help your child make positive Cyber Choices
Cyber Choices is co-ordinated by the National Crime Agency (NCA) and delivered by regional/local police teams. The aim is to explain the difference between legal and illegal cyber activity, encourage individuals to make informed choices about their use of technology, divert them away from cyber-crime and promote legal tech opportunities.
https://parentinfo.org/article/help-your-child-make-positive-cyber-choices

Woman who deliberately deleted firm's Dropbox is sentenced
A businesswoman from North Yorkshire has been sentenced for deleting thousands of important files from a company that went on to collapse.
https://northyorkshire.police.uk/news/businesswoman-sentenced/

When Security takes a Backseat to Productivity
https://krebsonsecurity.com/2020/06/when-security-takes-a-backseat-to-productivity/



TECH TALK

NCSC Weekly Threat Report Topics

- Poor password practices
- Email accounts targeted in phishing campaign
- US network outages cause widespread speculation
- Australia responds to targeting of government and critical infrastructure.

https://www.ncsc.gov.uk/report/weekly-threat-report-19th-june-2020

Mass Credential Harvesting Phishing Campaign

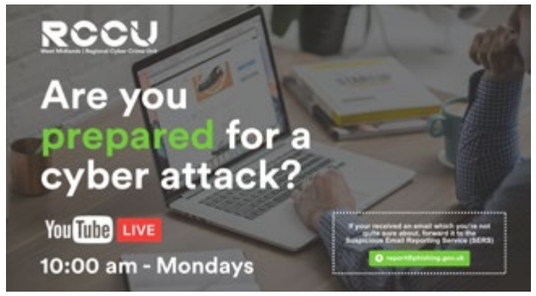
The NCSC has alerted organisations to a large scale phishing campaign looking to harvest account credentials. This is an ongoing campaign active in the UK, which started back in October 2019. The NCSC has provided technical mitigations which IT team's can implement to protect against this campaign in their latest alert.

The alert page also links to further resources on securing Office 365 accounts, improving your password use, and defending against phishing generally. This page can be found at

https://www.ncsc.gov.uk/news/mass-credential-harvesting-phishing-campaign-active-uk

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

ROCU
West Midlands | Regional Cyber Crime Unit
CYBER THREAT PODCAST

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/



WWW.WMCYBER.ORG

Cyber Crime Advice: All in one place

We are pleased to announce the launch of our new website

Offering both personal and business advice, the website has a wealth of information to help you stay safe onine. Get yourself protected against threats with our simple and easy tp use advice.

WM ROCU REGIONAL CYBER CRIME UNIT