Cyber Security Links and Advice

Provided by Chris White, (Police Cyber Security Advisor | Police Cyber Prevent Supervisor, South East Regional Organised Crime Unit) who presented to the MBF on 4th September 2018

Useful Websites

- **Small business guide provided by the National Cyber Security Centre**
  - https://www.ncsc.gov.uk/smallbusiness
- **10 steps to cyber security provided by the National Cyber Security Centre**
  - www.ncsc.gov.uk/guidance/10-steps-cyber-security
- **Weekly threat reports and alerts provided by the National Cyber Security Centre**
  - www.ncsc.gov.uk/index/report
- **Various infographics provided by the National Cyber Security Centre**
  - www.ncsc.gov.uk/information/infographics-ncsc
  - Small Business guide
  - Small charity guide
  - NCSC Glossary
  - Password Guidance
  - 10 steps to Cyber Security
  - Common Cyber Attacks
  - Bring Your Own Device Guidance
  - Managing Information Risk
- **The Little book of big scams from the Metropolitan Police Service**
  - https://www.met.police.uk/SysSiteAssets/media/downloads/advice/met/fraud/the-little-book-of-big-scams.pdf
- **The Little book of Cyber scams from the Metropolitan Police Service**
  - https://www.met.police.uk/SysSiteAssets/media/downloads/advice/met/fraud/little-book-of-cyberscams.pdf
- **The Little book of Big scams (Business Edition) from the Metropolitan Police Service**
  - https://www.met.police.uk/SysSiteAssets/media/downloads/advice/met/fraud/little-book-of-big-scams-business-edition.pdf
- **General advice on Cyber Security for Business & Public**
  - Cyber Aware www.cyberaware.gov.uk
  - Cyber Essentials www.cyberessentials.ncsc.gov.uk
  - Europol ransom free keys www.nomoreransom.org
- **Online safety on all area for everyone**
  - Get safe online www.getsafeonline.org
- **Online safety for under 18s, parents and schools :**
  - Net aware www.net-aware.org.uk
  - Think you Know www.thinkuknow.co.uk
  - UK Safer Internet Centre www.saferinternet.org.uk
  - NSPCC www.nspcc.org.uk
  - CEOP www.ceop.police.uk
- **How to setup devices safely**
  - Internet matters www.internetmatters.org

    - Two factor authentication www.turn2fa.com
- **Youtube Channels**
    - CEOP youtube channel
    - South East ROCU Cyber Protect
- **Check for latest frauds and scams:**
    - Action Fraud www.actionfraud.police.uk
- **Helpful Linkedin:**
    - South East ROCU Cyber Protect
- **Helpful Instagram:**
    - SECyberProtect
- **Helpful Twitter feeds:**
    - @GetSafeOnline
    - @cyberawaregov
    - @ncsc
    - @SECyberprotect
    - @cyberprotectUK
    - @TakeFive
- **Helpful Facebook feeds:**
    - www.facebook.com/cyberawaregov
    - www.facebook.com/takefivestopfraud
    - www.facebook.com/CyberProtectUK
    - www.facebook.com/SECyberProtect
- **If you look after a network please join the CISP platform**
    - https://www.ncsc.gov.uk/cisp
- **If you look after a public sector network please monitor your own domain**
    - https://www.webcheck.service.ncsc.gov.uk/

A bit of brain training for you…..

- **Phishing Emails and scams**
    - Everyday countless phishing emails and messages are sent to unsuspecting victims all over the world. Most of them look suspicious, but some of them can be a little more convincing, so how well do you know the difference between legitimate and phishing messages? There's a nice little quiz available online – it's quick and shouldn't take longer than 5 minutes…..Fingers crossed you get 8 out of 8!
    - https://takefive-stopfraud.org.uk/takethetest/
- **Are your details linked online to your employer, see what people can find out about you and your company, have a look?**
    - https://hunter.io/
- **Check to see if you have an email account that has been compromised in a data breach?**
    - www.haveibeenpwned.com
- **And if you are an administrator you can complete an organisational check?**
    - https://haveibeenpwned.com/DomainSearch
- **Check to see what the internet knows about you?**
    - www.pipl.com
- **Keep track of your credit score for free by signing up to one of the many service providers?**
    - www.Clearscore.com for example is one of the many providers
- **Make you passwords slightly more complex**
    - https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

    - Current best practice advises **THREE RANDOM WORDS**. Add complexity, convert some letters to numbers and add special characters
    - For example **BEACHBUCKETSPADE**, to add complexity **8EACH8UCK3TSP4DE£**
    - Your single most important account and password is your email – effectively, anyone taking control of your email can then reset all your other passwords locking you out.
    - Don't use words / names / information that may be in the public domain or easily worked out from social media content, such as Mum's maiden name; Date / Place of birth; pets names; teams you support etc…
    - Always change default passwords on all SMART devices/routers for your own unique one
    - ALWAYS log out of sites you have logged in to – especially on shared / public devices / machines
- **Make yourself more secure at home. A Secure Device (including mobile phones) means:**
    - an operating system and all applications with up to date software patches from their respective manufacturers;
    - an up to date browser
    - an installed fully operational anti-virus product with up to date configuration data;
    - an installed fully operational anti-spyware product with up to date configuration data
    - an installed operational firewall
    - enable 2 step factor authentication
    - an installed operational VPN
- **Look at your social media settings…**
    - Opt for "Friends only"
    - Be a good friend and change your settings to 'hide' your friends list to protect their security too. Also helps prevent account cloning issues
    - "closed" groups are often open to the public, even though a closed group requires admin approval to join!
    - Whenever Apple, Android or FB app updates, check your privacy settings to ensure they haven't reverted to the default "public" setting
    - Be mindful that "friends" settings can affect your own security. Your friend "Jack" may comment on your post, but depending on his settings, his friends may be able to see, comment on and potentially share your original post.
    - turn location settings off when you post to social media as it indicates your current location
    - Be mindful of regularly checking in to places as it highlights a pattern – also, remember 'checking in' is publicly viewable
    - Change Facebook settings make old Timeline posts visible only to you
    - Check that photos are not "publicly available"
    - Opt to approve photos and posts by others before they appear on your timeline
    - Spring clean and remove any posts that may not show you in a positive way
        - Delete any old social media accounts you no longer use