Cyber Byte

April 2022

Locking out Cyber Criminals.

Police Scotland Cybercrime Harm Prevention team would like to introduce this months Cyber Byte to provide you with awareness and information on how to help keep you and your family safe online.

COVID and lockdown caused us to rely more heavily on internet access and inter-connectivity than ever before and, as a lasting effect, we will continue to make advances in our use of this technology across all levels of business and age ranges from our children and young people to our Age communities.

As we surf the internet, we leave our digital footprint – this is a digital trace we leave on the sites we visit such as where we shop and the social media apps we browse. More often than not we have to log into these various sites with our email address and a password. Our passwords are like digital keys, they allow us to unlock our online accounts to access them.

So how many passwords or digital keys do you have? Is it just the one that you use for all your online accounts for convenience? Or do you have more than one password or digital key for all your different online accounts?

Another way of looking at it is by asking yourself "How many keys do I have to lock my house, shed, garage or car". The answer is that we use different keys to lock our property. Imagine if you just had one key and it was stolen, the criminal would be able to unlock all your property using that single key and that would be the same if you just have one single password for all your online accounts. So, having more than one password for your different online accounts is the safest way to protect them from being attacked and your data being stolen by Cyber criminals, especially your online banking, shopping, social media and email accounts.

Our partners at the NCSC (National Cyber Security Centre) have created excellent guidance on how to create unique passwords or even better using three random words as passwords. Three random word passwords are exactly what it says, three random words from what you are seeing around you just now – "**windowbirdtree**", "**hillcloudshower**", "**catbirdtable**" and by adding a special character and a number, what you create are unique passwords with no connection to what most peoples passwords relate to such as a favourite holiday destination, pets name, school or childrens' names, hobbies etc things which Cyber criminals can easily find out about you from social media.

You can find out more at;
Three random words - NCSC.GOV.UK

You should also consider applying another level of protection know as 2-step verification (2SV) on your accounts, which will prevent anyone accessing your accounts even if they know your password. The following link will support you through adding 2SV to your online accounts.

You can find out more at;
Turn on 2-step verification (2SV) - NCSC.GOV.UK

Data Breaches are very common and criminals can use the stolen information to carry out targeted phishing campaigns. Phishing emails can look very genuine, can be forceful in the manner they are written and be extremely persuasive. These can arrive as private emails or Smishing texts commonly pretending to be from a government department offering you a rebate or demanding something else and forcing you to act quickly out of fear, or it could be hinting you might have won something - but you cannot remember entering the competition.

Phishing emails can also relate to your work and these are usually asking for change of banking details or change in HR records to be done, getting a member of staff to do something they wouldn't normally do – so pause and consider and seek guidance before reacting or clicking on any links attached to such and email.

Our guidance is – Don't click on the links or reply to these emails but to report to your IT team if at your work, as they could also carry a malware, or you can report to the Police if you have responded and realised you have provided data.

Otherwise we would ask you to forward the email, even if you are not certain it's a scam, to the Suspicious Email Reporting Service or SERs. If you have not heard of the SERs before, this link will take you to the site; Report a scam email - NCSC.GOV.UK

- Received a suspicious text message? Forward it to 7726 on your mobile phone and this enables your provider to investigate.
- Both these services are free to use.

As of the 22nd February 2022 the number of Suspicious Email reported to the service is over 10 Million – this includes 76,000 scams removed from 139,000 URL's. Date site last visited 29/03/2022.

Information from Police Scotland Cybercrime Harm Prevention Team
PPCWCyberHarmPrevention@scotland.police.uk
All information was correct at time of distribution. 01/04/2022.