Eastern Region Special Operations Unit

Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Friday 1st May 2020

Today's topic is 'Passwords'.

The following advice is pertinent to both business and personal users of digital devices and online services. Laptops, computers, tablets and smartphones contain a lot of items such as business-critical data, customer information, personal information and details of online accounts.

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised users accessing your devices. Things to keep in mind when using passwords for personal or organisation devices and services:

- Make sure you switch on password protection - Set a screen lock password, PIN, or other authentication method (fingerprint or face unlock).
- Use Two-factor authentication (2FA) for important' accounts. - This requires two different methods to 'prove' your identity.
- Avoid using predictable passwords (Pa$$word123)
- Passwords should be easy to remember, but hard for somebody else to guess.
- IT systems should **not** require staff to share accounts or passwords to get their job done.
- Avoid password overload - Passwords only need to be changed when a compromise is suspected.
- Staff will forget passwords, so make sure they can reset their own passwords easily.
- If using password managers, make sure the master password is a strong one
- Change all default passwords.
- The most secure passwords are made up of three random words and can be further strengthened by adding numbers, capital letters and symbols, eg pink31Rainbowjam9!

Password 'Spraying'

One common way that online accounts are breached is through password spraying. Lists of a small number of common passwords are used to brute force large numbers of accounts.

These attacks are successful because for large set of users there will be some using very common passwords.

The NCSC recently conducted a research study which allowed participating organisations to assess how vulnerable they would be to a password spraying attack.

Results from the study:

- 75% had accounts with passwords featured in the top 1,000 passwords
- 87% had accounts with passwords that featured in the top 10,000

Whilst account lockout policies limit attackers trying multiple passwords against a single account, the account lockout counters usually reset over time, allowing persistent attackers to try hundreds or even thousands of common passwords.

One of the most effective ways to secure against these attacks is to prevent users from using common passwords in the first place. Using a password blacklist stops users choosing common passwords. More information on password blacklists can be found here.

How to create a strong memorable password - use three random words.
Numbers, symbols and Capital letters can still be added, e.g. **3RedHouseMonkeys27!**
Be creative and use words memorable to you, so that people can't guess your password. Your social media accounts can give away vital clues about yourself so don't use words such as your child's name or favorite sports team which are easy for people to guess.

Hot topics

A new flight refund scam that attempts to exploit the ongoing coronavirus outbreak has been reported. The phishing email includes a fake refund form which if filled in would provide scammers with personal information including names and card details.

Google saw more that 18 million daily malware and phishing emails relating to Covid19 last week, plus 240 million spam messages.

COVID-19 themed Email messages targeting executives and employees requesting the urgent wiring of funds to cover medical costs, purchase of gift cards to buy essentials online and the urgent update of banking details continue to increase.

Reporting

Reporting to Action Fraud can be done online or by calling 0300 123 2040.
To report offers of financial assistance from HMRC, contact phishing@hmrc.gov.uk.

This advice has been collated by the East Midlands Regional Organised Crime Unit (ROCU) and is intended for wider distribution to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the ERSOU Protect Team CyberProtect@ERSOU.pnn.police.uk or your local Force protect team.