Eastern Region Special Operations Unit

Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Wednesday 27th May 2020

Today's topic is 'Passwords'.

Passwords are nothing new, second century BC Greek historian Polybius, wrote about them. The Roman military used passwords to distinguish friend from foe. The tale "Ali Baba and the Forty Thieves," invented by Antoine Galland in the 18th century coined the passphrase "Open, Sesame!" to unlock a cave and is still used as a catchphrase today.

Fast forward a few centuries to 1960 and Fernando Corbató introduced the idea to computer science while working at the Massachusetts Institute of Technology (MIT). To keep individual files private, the password was developed so users could only access their own specific files for their allotted time - computer time was limited back in the 60s!

Today we use passwords to access personal computers and computing devices and services of all kinds. While protecting them from attackers who might read, steal or even destroy sensitive data.

Unfortunately, many of us find passwords difficult - we have multiple passwords to remember and are told that they must include digits, symbols and upper or lower case letters. Faced with such complexity, many will: use the same password for everything, use a password that is easily guessed or write passwords down.

Password tips:

Use three random words. This introduces so many permutations that the password is extremely difficult to crack. It also acts as a 'pass phrase', which is easier to remember. Finally, there is plenty of scope to add upper and lowercase letters or symbols with the words you can remember.

Use a strong separate password for your recovery email address and separate passwords for accounts and be mindful who is watching when entering passwords.

Usernames and passwords require us to 'know something'. However, we can also prove who we are by 'having something', such as a pin (token) sent to our phone. This is an example of 2 Step Factor Authentication. 2FA is secure and should be used for any sensitive or important operation.

Organisations could consider use of biometric security systems - facial recognition, fingerprint, palm and iris scans are generally considered the most secure form of authentication, when combined with 'something you know' (password) or 'have' (token) as 2 factor authentication.

Alternatively, a credential manager can be a wise investment. They can generate complex passwords using a range of rules and auto complete forms. However, setting them up can take time and the master password (to open the credential manager) must be complex.

System administrators should:

- Change all default passwords on any IT system or hardware.
- Prevent users choosing well known passwords by configuring a 'password deny list'.

- Use a progressive time delay between each successive login attempt. This gives the employee a chance to remember credentials, whilst minimising the costs associated with account recovery. Alternatively, limit 'login' attempts before locking accounts.
- Log successive failed password attempts; attempts from unexpected geographical areas and reports of unexpected account lockouts.
- Consider single sign on technology but make sure that any corporate web apps use HTTPS when communicating with such systems. This will protect credentials or 'authorisation tokens' from illegitimate access as they travel over public networks.
- Salt and then hash passwords stored on business systems. A salt will add random characters to a password and the hash will turn the password into an unreadable string of characters, making it more difficult to steal.

More detailed guidance on passwords, from the NCSC, can be found here

Hot Topics

Pizza-Hut have identified that scammers are taking advantage of the COVID-19 lockdown to set up multiple fake sites using its brand name to lure the unsuspecting into giving bank/card details. The addresses of the fake sites — which strongly resemble the authentic Pizza Hut web-based ordering platform — include 'http://pizzahutaccount.com' and 'http://pizzahut-service.co.uk'.

The UK National Cyber Security Centre (NCSC) and the US Cybersecurity and Infrastructure Security Agency (CISA) have released a joint advisory concerning the targeting of coronavirus response organisations. Healthcare bodies, medical research organisations, pharmaceutical companies, academia, and local governments have been targeted. Most of these attacks used password spraying to gain access to a large number of accounts.

TV Licensing scam emails, in which the recipient is advised they are eligible for six months of free TV Licensing, due to COVID-19, also claim the recipient's payment has failed and they need to renew now in order to avoid prosecution.

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.