Passwords

Passwords are our last line of defence against an attacker, however the majority of users are reusing insecure passwords across multiple accounts they own. This can have catastrophic consequences for users and therefore different passwords should always be used.

- Use a different, long password for every account
- A password manager can help you create and store passwords

How do hackers obtain passwords?

There are numerous ways passwords are "hacked": phishing emails with a link to a fake website which lures people into entering their password, guessing easy passwords like Password1! and finding username and password combinations dumped on the internet by other hackers are the most common.

Out biggest problem

Reusing the same password across multiple sites is the biggest problem for password security. Cyber-criminals crawl the internet for any username and password information which is published on the internet by other cyber-criminals. They then try this username and password combination on every single site they can think of. For example, if you use the same password on your iCloud account as you do on a travel forum and the travel forum gets hacked, then cyber criminals can try that combination on iCloud and have access to your contacts, photos and other sensitive information.

Generating secure passwords

A common misconception is that complexity is critical to password security. The result of this is passwords containing complex sequences which are difficult to remember. Using a phrase is easier to remember and type. For example "T4ylOrSw1ft" as a password is not as strong as "Taylor swift is brilliant!". The length of a password gives strength, not the complexity. All passwords should be a minimum of 16 characters.

Managing passwords safely

Password managers can help to create strong, unique passwords for each site. A password manager is effectively a safe which contains all of your login details for the sites you use. This safe is protected by a single "master password" which must be very strong. To log into a site, you need to access the safe which can then autofill the password for you. Although this can be seen as putting all your eggs in one basket, the reason for using a password manager is to avoid weak passwords being used and re-used. 1Password and Lastpass are examples of password managers.

//curious frank:

www.curious-frank.com

A division of the Scottish Business Resilience Centre