NEBRC
NORTH EAST BUSINESS RESILIENCE CENTRE
CRIME PREVENTION IN A DIGITAL ERA

PASSWORDS

Passwords are often our only line of defence against an attacker. Unfortunately, most people re-use the same password for most of their accounts. This re-use can have catastrophic consequences for the security of your online accounts.

Use a different password for every account.

Use a password manager to help you store and create passwords.

How do attackers obtain your password?

The most common method is finding it in data dumps from websites which other hackers have compromised. Attackers can also research you via social media and attempt to guess your password. Your dog's name followed by your year of birth (e.g. patch 1969) is not a good password. An attacker can easily find out your dog's name and year of birth.

Password re-use

This is our biggest problem. Re-using the same password across multiple accounts will result in you having an account compromised. For example, you use the same password on your iCloud account and a travel forum. When the travel forum is compromised, your password is now public knowledge. The attackers will take the email address and password from the travel forum and try to log in to any service they think you use. Now, because you re-used your password, the attacker has access to your iCloud account.

Generating secure passphrases

The latest advice from the NCSC on generating a secure pasword is to use three random words. You just put them together, like 'coffeetrainfish' (this is an example, do not use this as your actual password). You can choose words that are memorable, but should avoid those that will be easy to guess, such as the names of family members or pets. You can also use spaces or punctuation between the words to make your password even more secure.

Password managers

Password managers are special pieces of software which store all your usernames and passwords. Think of them as bank vaults. We store all our valuables in one very secure place, protected with a strong vault door. In this case, the vault door is your "master password" which unlocks your password manager. Anytime you need to log in to a site, you unlock your password manager and copy and paste the password into the website. Much more convenient than trying to look up the password in your little black book or trying to remember which variation of your password you used for a specific site. While this is an "all your eggs in one basket" approach, the basket is very secure. It is highly likely that you will be compromised because of password re-use. It is far less likely that your password manager will be compromised.