fiscal engineers™
money. life. balance.

The 3 top cyber threats

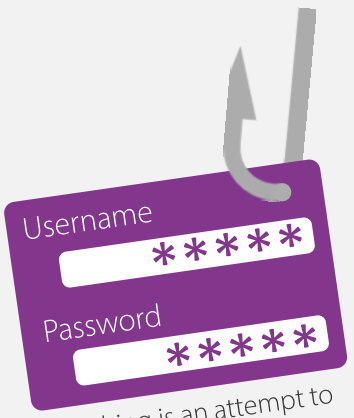
Brute Force Attacks

A method used to steal an account password. Hackers take a username (such as an email address) and use an automated service to try thousands of the most commonly used passwords all at once with that username.

Public WiFi

Free WiFi in public spaces offer very limited protection as there are many tools that can be used to intercept data going between the WiFi and its connected devices. Generally speaking, mobile data use is much more safe.

Phishing Attacks



Phishing is an attempt to steal sensitive information under the guise of a trustworthy source, usually by way of emails

Frequent

Bulk phishing – the most used and a 'hit it and hope' approach. These emails are circulated to mass mailing groups and will likely address you generically, such as 'Dear Sir/Madam', 'Apple User' or 'Account holder'. Bulk phishing is easier to spot, particularly when you don't have an account with the supposed sender.

infrequent

Spear phishing – adopts a more direct approach by using previously gathered personal data from global data breaches such as TalkTalk (2015) or from data entered in unprotected websites to increase authenticity. These emails may address you by your full name or may even cite a password you have previously used.

Rare

Clone phishing – this type requires unauthorised access to a mailbox. The attacker will 'clone' an already existing email and assume the identity of the original sender, replacing any hyperlinks, attachments or personal information (such as bank details) with malicious versions in all future correspondence.

How can you better protect yourself?

Password Security

1

Use a pass 'phrase', not a pass 'word' and include a combination of lower/uppercase letters, numbers and symbols. This could be your favourite song, film or catch-phrase.

Password Management

2

Avoid reusing passwords or passphrases. Think about how you can use the same core password, but add additional characters to make each one individual.

Email awareness

3

Avoid clicking on any attachments or links in suspicious emails and delete it. If you're unsure whether an email has come from the assumed sender, give them a call to be sure.

Antivirus protection

4

You must have antivirus software installed on all laptops or desktop computers. Mobile devices have antivirus protection integrated which is why they should always be updated.

Update, update, update

5

Always choose to install updates as soon as they're available. Updates nearly always include security fixes so it's important to keep your mobile devices, computers and applications up-to-date.

Secure mobile device access

6

Protect your data by making sure that every device you own requires password/pin code/biometric authentication to be unlocked.