Protecting your pa$$w*rd$

> While some cyberattacks are intricate and sophisticated, the vast majority start with criminals taking advantage of a relatively small vulnerability, whether unpatched system software or an employee who isn't paying quite enough attention.

Time and time again, we learn that a lack of basic cybersecurity hygiene is where some businesses come unstuck.

One of those basics is having strong and unique passwords across vital business systems. Here, we've outlined a few ways hackers crack passwords and what you can do to stop them.

How hackers get their hands on passwords...

Brute force attacks

Sometimes it's easier to let the computer do the work. This method involves a program trying different username and password combinations in quick succession.

Poor password storage

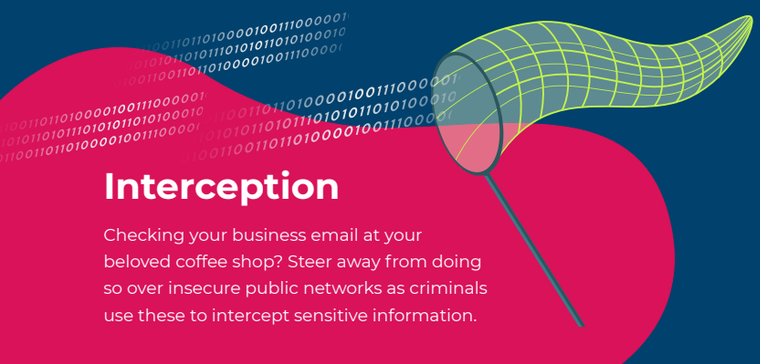
Using a sticky note to remember your password? Beware. This could leave you wide open to attack should it get into the wrong hands. What's more, be careful storing passwords electronically as criminals already in your system can search file structures for passwords that could enable broader access.

Dark web leaks

The reason why we advise never to use the same password twice is because once it's leaked on the dark web once, it can be used to gain access to other, often more valuable websites and systems.

Social engineering

Humans tend to be one of the weaker links in the cybersecurity chain. Criminals often lure individuals into willingly handing over passwords though fake emails, landing pages, and more.



Interception

Checking your business email at your beloved coffee shop? Steer away from doing so over insecure public networks as criminals use these to intercept sensitive information.

And how you can stay more secure...

- Use password managers to encourage the usage of complex and unique passwords
- Only use passwords where needed to avoid password overload
- Don't require frequent password changes unless there's evidence it has been compromised
- Encourage the use of passphrases rather than passwords, as they are easier to remember
- Require complex passwords using upper and lowercase, special symbols, and numbers
- Encourage users to never re-use passwords between work and home
- Store passwords securely in an encrypted format
- Change all default and vendor-supplied passwords before deployment

Want more information? Reach out to cybermarketing@cfc.com