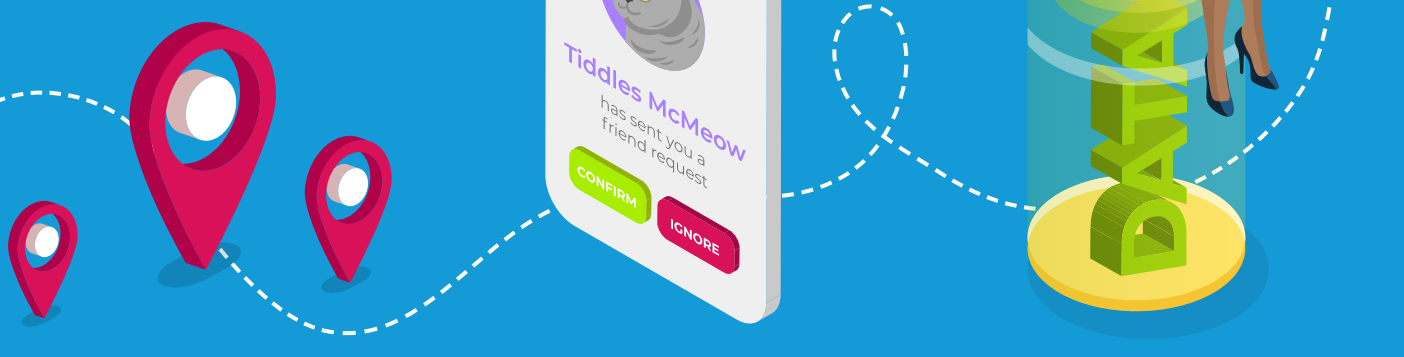
How to stay safe online

The CFC Incident Response team has seen a surge in cyber events affecting businesses of all sizes. With the growing volume and sophistication of online threats like viruses, ransomware, and phishing scams, it's important to know the proper practices to stay safe online.

Be responsible



Beware of app permissions

A tracking app may want to know your location, but a gaming app doesn't need that information. Only give permissions to the applications that need them. Don't be afraid to deny permissions to apps.

Do you really know your 'friends'?

A good way to keep yourself and your information safe is to only accept friend requests from people you know personally and ensure social media accounts are set to private. This will limit the amount of information available to the public.

Keep a lid on your data

When you log into any account using a third-party app like Facebook, information is being shared between the third-party app and your account. Don't allow applications to share your data by using unique logins for each.

Computers need vaccinations too

Every device needs antivirus software. If you end up downloading a malicious application, or an application becomes infected, antivirus software will help to secure the device and remove the infection.

Lockdown

Enabling a lock screen and encrypting your device gives you peace of mind if your device is stolen as it is unlikely the attacker will know your password and be able to gain access to your data.

Syncing ship

Turning off auto-sync forces an attacker who's stolen your device to enter your password, which will stop an individual who doesn't know it.

Don't share if you care

It's very common to share your life on social media, but what you share can be used against you, and it's notoriously difficult to permanently delete information posted online. An attacker can impersonate you, gain important information about you, or hack into your accounts on multiple sites.

Reliable apps

Choose apps from a reputable developer and download only from official app stores. This will reduce the risk of installing a malicious application to your device. Also, if an app has a large number of five-star ratings but no reviews, it could be malicious and you should be cautious.

Be secure

The more complex, the better

Relatively short passwords are less secure and make it easier for hackers to break. It is recommended that passwords be anywhere between 8 to 64 characters long. Though your own company's regulations may differ, it has been advised that forcing users to include lots of symbols and numbers doesn't always increase password security. Concentrate on length and memorability instead.

Sentences make it easier

Is it possible to remember a 64 character password? It is if you think in sentences, not words. A sentence is easier to remember than a made-up combination of letters and numbers, and provides the all-important length to make it more difficult to crack.

S for Secure

A legitimate shopping site is likely to be using HTTPS rather than HTTP. Ensure the URL includes HTTPS and a lock icon in the corner.

Slow it down

If someone is insistent you to take action right now, slow down the communication. Ask questions and check with people you trust. If you can't confirm that it's legitimate, ask another trustworthy person.

Don't reuse passwords

Passwords are constantly being cracked or exfiltrated through data breaches and added to a database of passwords to use in the future attacks. Always use strong unique passwords to be safe.

What you know, what you have and what you are

There are three different factors to think about when securing an account: what you know, what you have and what you are. Mixing these factors will give you stronger protection. If someone has stolen your password but not your mobile phone, they cannot gain access.

The benefit of biometrics

Biometric authentication includes a fingerprint, palm or scanning your iris. Consider implementing biometrics where possible to provide an extra layer of security.

Sounds too good

Phishers feed on mistakes. They will offer you quick wins or incredible deals to get you to make a thoughtless decision. Ask yourself "Does this sound too good to be true?"

Watch out for the scam

A product or service may look appealing on a webpage, but how do you know the site is genuine? Consumer watchdogs like the Better Business Bureau can help you check if a business is genuine.

Multi-factor authentication

Having multi-factor authentication enabled on account logins makes it more difficult for attackers to gain unauthorised access to your account. We suggest always implementing MFA where available.

Think before you click on the link

Links in emails can be spoofed, making you think you're going to a site you aren't. Double check the link by hovering over the URL.

Be protected

Fail to license, license to fail

You should never use cracked, pirated or unlicensed versions of software or an OS. These commonly contain malware which can easily infect your device when installed and is also against the law.

Patch early, patch often

It is important to keep your system updated. Updating often will fix bugs, patch vulnerabilities as soon as a fix is available, and keep your system optimised. Attackers are always finding new ways to infiltrate a system, so it's important you keep up with these changes.

Spot the fake

It is possible for an attacker to create a clone of a network with the same or similar name to a legitimate private network. These clones will not be password protected to lure people into connecting to them. Always get confirmation when attempting to connect to Wi-Fi in public.

Auto-connect is incorrect

Allowing devices to automatically connect to known network is an easy method in allowing an attacker to infect your device. Disable auto-connect and be careful when connecting to a public network.

No privacy in public

Using public networks is always a risk. When using a public network in places such as a coffee shop, you should never access your sensitive information like your bank account. An attacker could intercept this data by monitoring the network.

Use official sources

Software updates should only be performed through an official source. Auto-updates are preferrable, but if they are unavailable, ensure the manufacturer's website is frequently checked for updates.

Are they authorized?

Never let someone else access sensitive data unless they are explicitly authorized, their identity has been proven, and they know the guidelines around the handling of that data. Impostors may try to tell you a good story, but that data represents a person's life and safety.

Protection

Customer's data should always be protected. Physical copies should be held in a secure location and digital data should be encrypted or password protected.

Limit what you carry

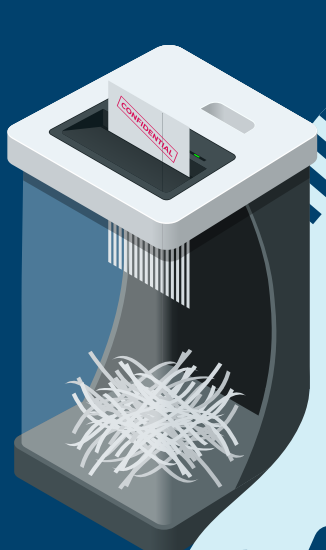
The less data you have stored on your person, the less can be lost or stolen. In the event of a data breach, there is less danger for clients.

Browser warning

A fake warning may ask you to download 'the latest software update' or fill in a form. However, a legitimate browser warning will ask to not do something, e.g. 'Back to safety'

Physical security

To keep data protected, physical security measures should be put in place. These include locks, badge checks, and confirming that individuals are authorized to access the area.



Shredded and erased

If customer information is no longer needed, the correct steps should be followed to ensure it is destroyed. Papers should be shredded and digital devices such as hard drives should be thoroughly erased.

For more information about cyber risk in insurance, visit our website, or contact our in-house cyber incident response team at cyberservices@cfcunderwriting.com.