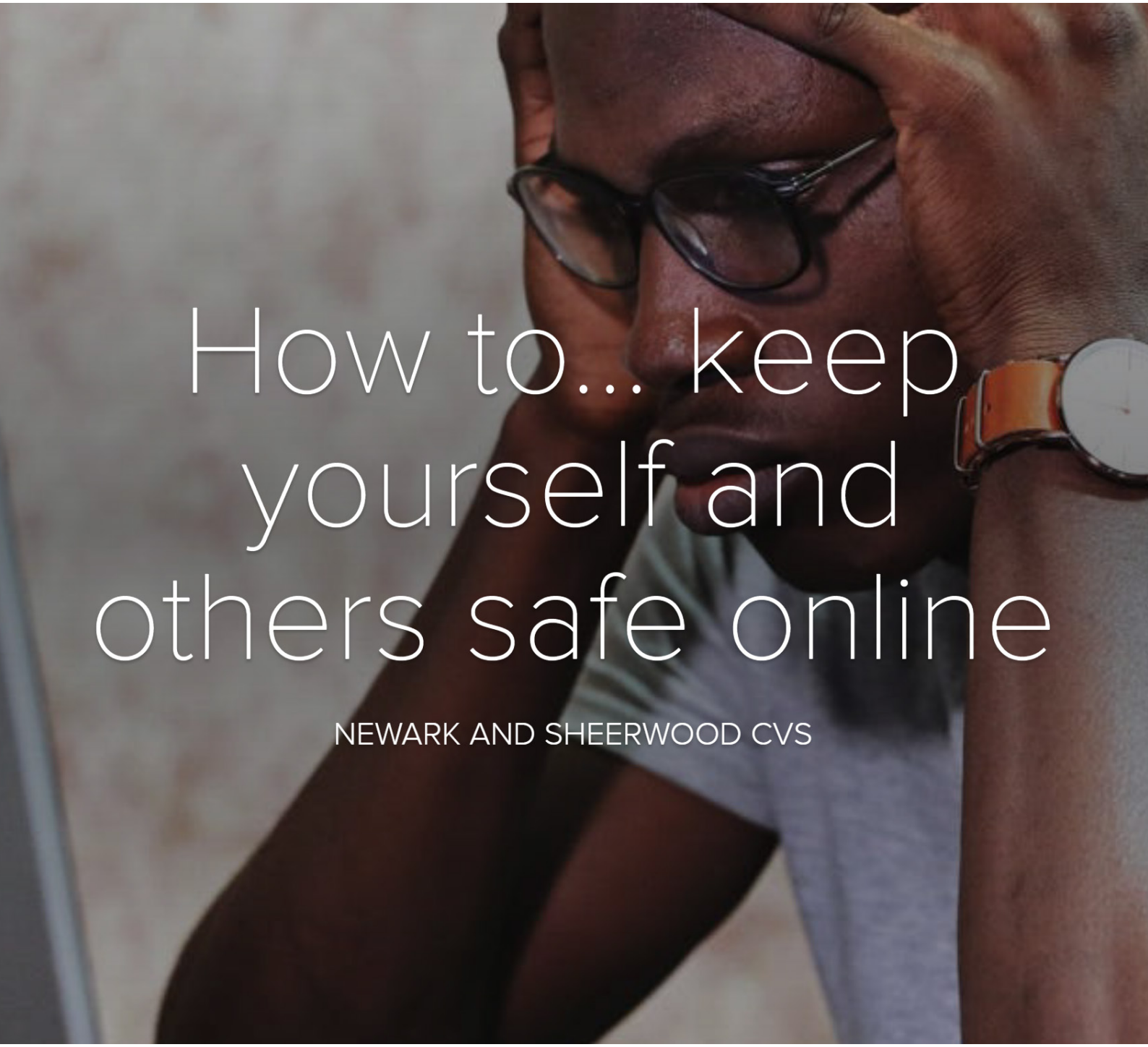


How to... keep yourself and others safe online

NEWARK AND SHEERWOOD CVS

This “how to” session is a part of our digital training webinar series, where we aim to help empower groups to explore the digital landscape, and discover the best way to meet their needs.

Webinar 45 minutes	Q&A portion

Today’s session will be a 45minute webinar, followed by a 15-minute Q&A session – where you will be able to ask questions related to the session.

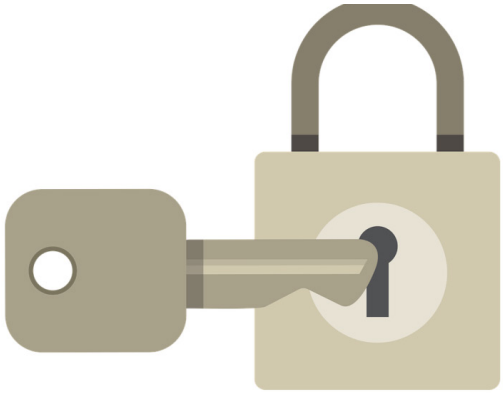
The internet is an amazing tool, with endless possibilities. However, an online presence can come with a few potential dangers that you need to be aware of, in order to keep yourself and others safe.

Today we will go through how to ensure you have security measures put in place when using the internet, including social media, public WIFI, email and messaging applications.

Personal account security

Passwords are a large part of maintaining security on the internet. Keep passwords secure by using 3 random words, mixed in with numbers and symbols, for example: '3Redhouse!pug27'

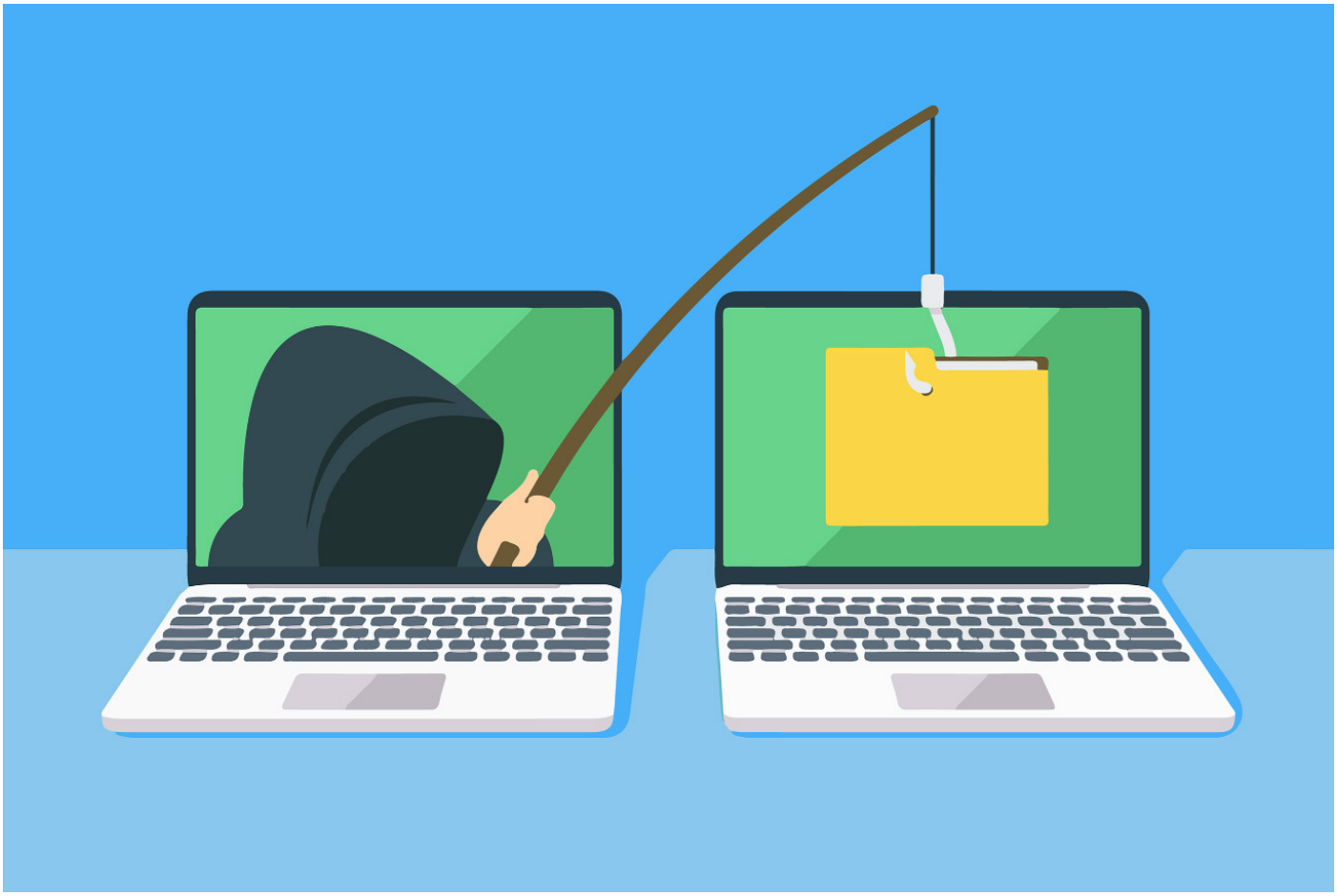
The key to creating a password is to not use information that can be easily linked back to yourself. Such as your name, your birthday, or information that could be in the public domain or on social media.



Password top tips

Passwords are a large part of maintaining security on the internet. Keep passwords secure by using 3 random words, mixed in with numbers and symbols, for example: '3Redhouse!pug27'

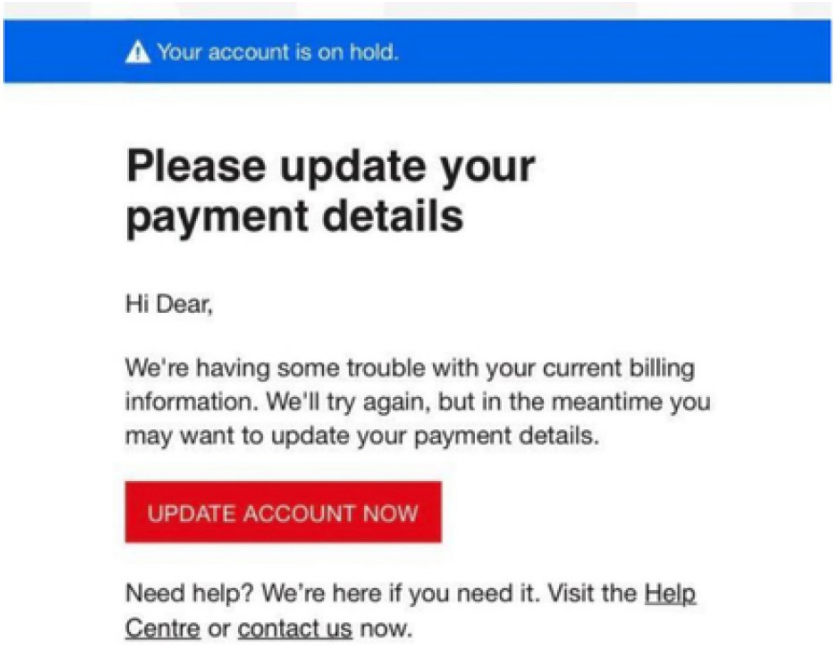
- Don’t use the same password on multiple accounts
- Change any default passwords as quickly as possible
- Use a mix of letters (ABC), numbers (123), and symbols (!*&^)



Phishing scams email and text

Be careful with any unexpected emails or text messages, even if the sender is known to you or looks like a previous message chain. Phishing messages are intended to look like they are from a legitimate source - to trick the reader into parting with sensitive data, or the messages may contain malware.

Phishing scams include spam emails, fake “free” offers, click bait, online quizzes and more. These tactics are to entice you to click on harmful links or hand over your personal information.



Tricking users is unfortunately how many scams are carried out, by using an alias to gain trust and then taking advantage. Make sure that you are cautious of suspicious messages. Genuine companies will not ask you to divulge sensitive information via email, text or over the phone. If in doubt, search the organisation's contact telephone number and call them directly to enquire about the email or text you have received.

Never respond directly to messages asking for your personal or financial details. Do not click on links or attachments; contact the apparent sender directly via a trusted source, for example their customer support, which will be listed on the official website. If the message is from your bank, contact them using the phone number on the back of your card. If phishing emails are becoming a major issue, you should consider creating a new email account.

WIFI

There is a difference between the security of the WIFI in your home and the WIFI in a public domain. You cannot be certain that public WIFI networks are secure, for example in places like cafes or hotels. Never use them to do anything confidential like making a payment. Criminals could intercept these transactions, steal your information, access files on your computer, or infect your device with malware. Where possible, use your mobile network internet, which will have built-in security.

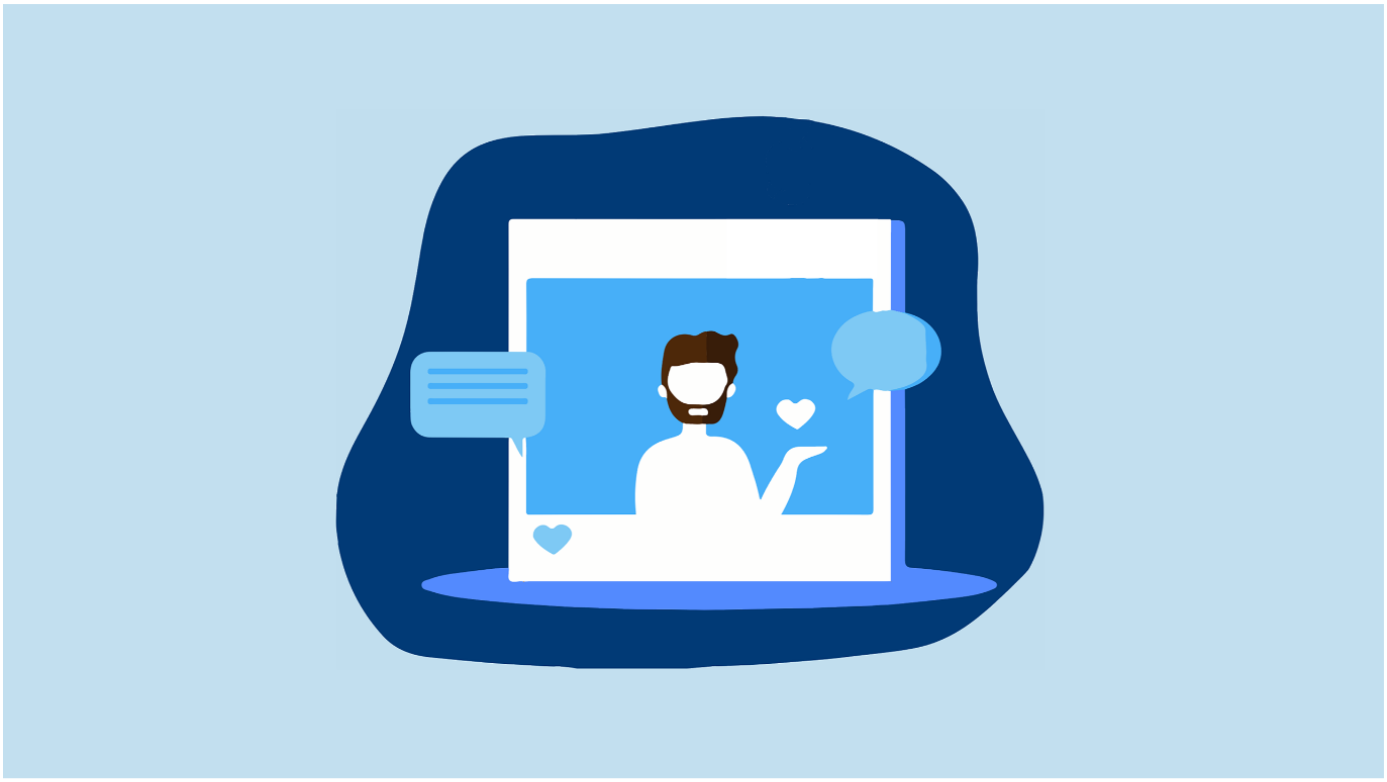
Antivirus

All devices should all have antivirus software regardless of what machine you are using. Ensure it is installed, updated regularly and running on the computers or devices that you are using.

The antivirus that I use and recommend is called Malwarebytes Anti-malware. It is a free program that scans your computer for potential threats and alerts you

to them. To learn further about anti-virus software, you can visit: https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product

Back up any important data to stop any loss of files if your device breaks, gets lost, stolen or is infected by malware. This can be a physical backup, like on a USB stick or on the cloud. Before disposing of any device, ensure you have performed a factory reset - to wipe all of your personal information.



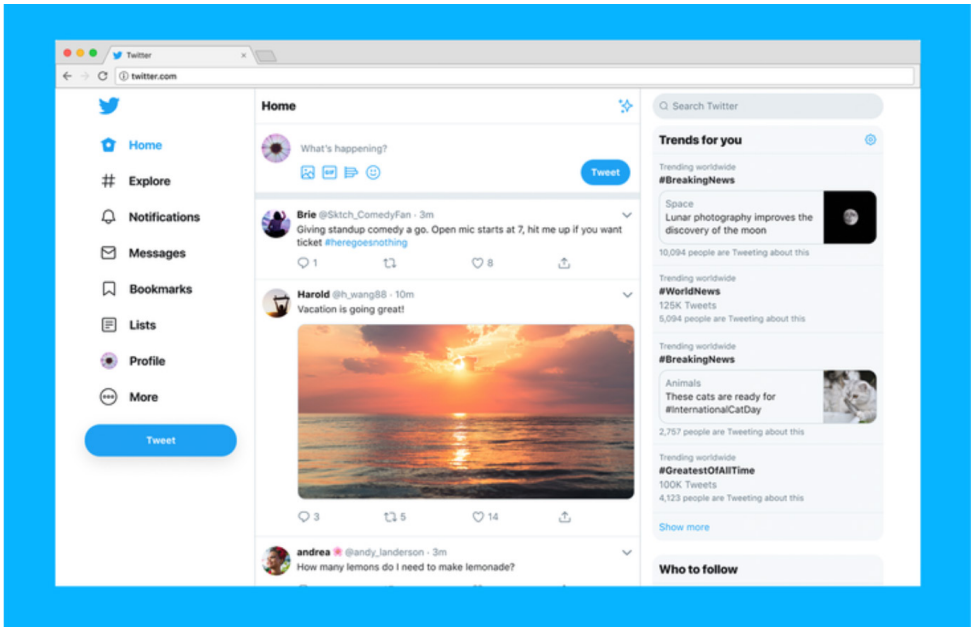
Security on Social Media

It is important when considering safety online, to think about what personal information you have shared 'publicly'. Think about what personal information is stored within your account, and what data you may have shared that could compromise you. For example, if you have liked a particular bank on social media, that could be an indicator of who you personally bank with.

To keep your social media pages private, make sure you have strong privacy settings. Choose ‘friends only’ or ‘only me’ when choosing your security settings. You can edit this by going into your profile or settings on the website or app.

Having private accounts is a great way to stop general social media users from being able to see any other information than your name.

Be careful when checking in and letting the world know your location. This can allow a criminal to work out patterns of behaviours, which could compromise your home and online security. My advice is that you are okay to geotag your location or post your holiday photos, just do it once you are home so you aren't vulnerable to people knowing your location.



There is the option to approve who follows you and who can tag you, which puts you in control of what happens on your account. If someone is trying to contact you via social media, and you do not want them to see your account, there is always the option to block them. By doing this, it ensures that they can no longer see your social media page or contact you via that platform.

Email

Email is incredibly useful, but there are a few potential dangers to look out for. It is important to always keep your data safe.

- Don't open links or attachments from email addresses you do not know or recognise. They may be unsafe or fraudulent
- If you are unsure whether a link may be fraudulent, type the website into a search engine, to make sure you are accessing the website securely
- Don’t forward or respond to emails you suspect of being unsafe or fraudulent.

Emails may even come from an email address that you recognise, such as a friend or family member. This can happen when someone's account is 'hacked'. If you receive something and it seems suspicious or out of character, give the person a ring to see if they sent it.

What to do if your financial details are compromised

Contact your bank or credit card directly and they will be able to help you. If possible, call via your mobile banking app or call the number on the back of your card.

Protecting people in an online group space

Private groups are places for people to come together to share or communicate on a range of personal topics. They are useful for organisations or groups, for example a peer support group.

Have a clear set of rules that people in the group need to follow. It is also a good idea to nominate a group moderator that can make sure content is appropriate and authentic.

WhatsApp groups are generally more secure as each profile has to be tied to a phone number. Make sure that the administrator of the group has the correct contact information for individuals being added.

In Facebook you can set up private groups for your organisation or group. This feature is useful for keeping group information private.

Another safety benefit is that users will have to request to be added to the group. The administrator for the group will need to authorise any requests, providing an opportunity to view the person's profile.

There is also the option to report a person or a post on Facebook if their content or actions are improper. This will trigger an investigation and the profile or post will be reviewed.

Top tips revisited

1. Create complex passwords. Creating strong, unique passwords for your accounts is an effective way of keeping your personal and financial information safe. Never share your passwords!

2. Boost your security. Once your logins are safe, make sure that your connections are secure. When at home or work, use a password-protected router that encrypts your data.

3. Click smart. Make sure that you don't invite danger with careless clicking. Many of today's online threats are based on phishing or social engineering, tricking you to divulge personal or sensitive information for fraudulent purposes.

4. Be selective with what you share. These days, there are a lot of opportunities to share our personal information online. Be cautious about what you share, particularly when it comes to your personal identity. This can be used to impersonate you or guess your passwords and logins.

5. Protect your mobile. Our mobile devices can be just as vulnerable to online threats as our laptops. In fact, mobile devices face new risks, such as fake apps and malicious links sent via text. Be careful where you click, do not respond to messages from strangers, and only download apps from official app stores.

6. Practice safe internet use. When shopping online or visiting websites for online banking/sensitive transactions, always make sure that the site's address has a padlock icon in the URL field. This indicates that the website is secure, and uses encryption to scramble your data so it cannot be intercepted by others.

7. Keep up to date. Keep all your software updated with the latest security patches. Turn on automatic updates, so you do not have to remember to manual update.

Thank you very much for attending. We now have time for some questions and answers. If anyone has something they would like to ask, just type your question into the Zoom Q&A panel.