THE UNIVERSITY OF THE THIRD AGE

Ringmer U3A Computer Group

Staying Safe On-line

Most of us use the Internet more and more despite the many frustrations. At present 95% of our members are on the web. However, many struggle to stay safe on-line. There are many pitfalls some of which can cause us to lose money. Ringmer U3A has consulted a Police Cyber Security Adviser in order to produce the advice given in this leaflet. Hopefully it will help you to make the most of everything the Internet has to offer whilst staying safe. Please do read it carefully then complete Your Check List at the end. We have provide links to the web sites.

Everyday countless phishing emails and messages are sent to unsuspecting victims.

Most of them look suspicious, but some of them can be a little more convincing, so how well do you know the difference between legitimate and phishing messages? There's a nice little **quiz available online** – it's quick and shouldn't take longer than 5 minutes…..

https://takefive-stopfraud.org.uk/takethetest/

Get Safe Online

is the UK's leading source of unbiased, factual and easy-to-understand information on online safety

Get Safe Online
Free expert advice

www.getsafeonline.org

Check to see if you have an email account that has been compromised in a data breach?
www.haveibeenpwned.com

Check to see what the internet knows about you? www.pipl.com

Why not **register** on the "In the Know - Surrey & Sussex" website
https://www.intheknow.community.

In the know Surrey and Sussex

Make yourself more secure. A Secure Device means an:

1. operating system and all applications with **up-to-date software patches** from their respective manufacturers;
2. **up-to-date browser**;
3. Installed & fully operational **anti-virus** product with up-to-date configuration data;
4. Installed & fully operational **anti-spyware** product with up-to-date configuration data;
5. and an installed operational **firewall.**

Make your passwords slightly more complex

- Current best practice advises **three random words**.
- **Add complexity** eg change BEACHBUCKETSPADE to 8EACH8UCK3TSP4DE£ .
- **Your most important account and password is your email** – effectively, anyone taking control of your email can then reset all your other passwords locking you out.
- **Don't use** words / names / information that may be in the public domain or easily worked out from social media content, such as Mum's maiden name; Date / Place of birth; pets names; teams you support etc…
- **Always change all default passwords** for your own unique one.
- **Always log out** of sites you have logged in to.

https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

Compiled by Ringmer U3A with advice from a Police Cyber Security Adviser

Staying Safe On-line

Look at your social media settings...

- Opt for “Friends only”.
- Be a good friend and change your settings to ‘hide’ your friends list to protect their security too. This also helps prevent account cloning issues.
- “closed” groups are often open to the public, even though a closed group requires admin approval to join!
- Whenever Apple, Android or FaceBook app updates, check your privacy settings to ensure they haven’t reverted to the default “public” setting.
- Be mindful that “friends” settings can affect your own security. Your friend “Jack” may comment on your post, but depending on his settings, his friends may be able to see, comment on and potentially share your original post.
- location settings off when you post to social media as it indicates your current location.
- Be mindful of regularly checking in to places as it highlights a pattern – also, remember ‘checking in’ is publicly viewable.
- Change Facebook settings to make old Timeline posts visible only to you.
- Check that photos are not “publicly available”.
- Opt to approve photos and posts by others before they appear on your timeline.
- Spring clean and remove any posts that may not show you in a positive way.
- Delete any old social media accounts you no longer use.

Watch out for Scams....

Big scams: https://www.met.police.uk/globalassets/downloads/fraud/the-little-book-of-big-scams.pdf

Cyber Scams: https://www.met.police.uk/globalassets/downloads/fraud/little-book-of-cyberscams.pdf

Report frauds and Scams: www.actionfraud.police.uk or phone **0300 123 2040**.

See extracts below and over the page from The Little Book of Big Scams.

Important information for all UK Bank Customers

Fraudsters are increasingly targeting consumers over the telephone, posing as bank staff, police officers and other officials and companies in a position of trust. Often the fraudster will claim that there has been fraud on your account and that you need to take action. You bank or the police will never:

- Phone you to ask for your 4-digit card PIN or your online banking password, even by tapping them into your phone key pad.
- Ask you to withdraw money to hand over to them for safe keeping.
- Ask you to transfer money to a new bank account for fraud reasons, even if they say that it is in your name.
- Send someone to your home to collect cash, PIN, payment card or cheque book even if you are a victim of fraud.
- Ask you to purchase goods by using your card and then hand them over for safe keeping.

Further guidance is given in The Little Book of Big Scams at

https://www.met.police.uk/globalassets/downloads/fraud/the-little-book-of-big-scams.pdf

Also see advice at https://takefive-stopfraud.org.uk/

Compiled by Ringmer U3A with advice from a Police Cyber Security Adviser

Staying Safe On-line

10 Golden Rules against Scams

Remember these 10 golden rules to help you beat the scammers.

1. Be suspicious of all 'Too good to be true' offers and deals. There are no guaranteed get-rich-quick schemes.
2. Do not agree to offers or deals immediately. Insist on time to obtain independent/legal advice before making a decision.
3. Do not hand over money or sign anything until you have checked the credentials of the company or individual.
4. Never send money to anyone you do not know or trust, whether in the UK or abroad, or use methods of payment that you are not comfortable with.
5. Never give banking or personal details to anyone you do not know or trust. This information is valuable so make sure you protect it.
6. Always log on to a website directly rather than clicking on links provided in an email.
7. Do not rely solely on glowing testimonials: find solid independent evidence of a company's success.
8. Always get independent/legal advice if an offer involves money, time or commitment.
9. If you spot a scam or have been scammed, report it and get help. Contact ActionFraud on 0300 123 2040 or online at www.actionfraud.police.uk Contact the Police if the suspect is known or still in the area.
10. Do not be embarrassed to report a scam. Because the scammers are cunning and clever there is no shame in being deceived. By reporting you will make it more difficult for them to deceive others.

Your Check List

- ☐ Up-to-date software patches?
- ☐ Anti-Spyware?
- ☐ Social Media settings?
- ☐ Up-to-date browser?
- ☐ Firewall?
- ☐ Register with "In the Know".
- ☐ More complex Passwords?
- ☐ Anti-virus?

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Remember

Don't open the attachments in any unsolicited emails you receive.

Don't click on the links within any unsolicited emails you receive.

Never respond to emails that ask for your personal or financial details.

Think twice before sharing information on-line.

Compiled by Ringmer U3A with advice from a Police Cyber Security Adviser