Cybercrime - Protect yourself from becoming a victim

(Article for inclusion on U3A website – 25 April 2017)

Brian Taylor (Chair)

If you recently received a text message or email purporting to be from Her Majesty's Revenue and Customs (HMRC) to say that you are eligible for a tax rebate, then beware! The message is bogus, a scam. It's an attempt to get your bank details and then use those details to remove cash from your account. Basically, it is one example of cybercrime fraud.

We live in an information-saturated society, a digital age of smartphones, 24 hour media and ever expanding connectivity. Internet use, sending/receiving emails, internet banking and the use of social media is part of modern life. Whilst technological progress has affected the way we live, work and do business, it also provides opportunities for criminals.

Cybercrime is now one of the most common offences in the United Kingdom. The Office for National Statistics (ONS) figures show that there were an estimated two million cybercrime offences in 2016, compared to 686,000 house burglary offences.

Criminals often target individuals by email or text, asking for security information and personal details, including bank details. This is known as 'Phishing'.

In addition to the HMRC tax rebate scam, another which is currently popular relates to parking fine letters. Victims have been receiving letters from scammers claiming to be the police/parking authorities, informing them they have been spotted illegally parking and have to pay a fine. There are many other scams, but all have the same objective - to steal your money.

Don't be caught out!

It's important to be aware of the action we can take to avoid becoming a victim. The National Crime Agency (NCA) and other authorities have issued some useful advice:

- No bank, financial institution or card issuer will contact you by email or text and ask you to enter your personal and financial details online, or to click on a link and confirm your bank details. If you receive this type of message, report it to your bank, then delete it. *Offers that look too good to be true usually are.*
- If you get an email from an unknown source, do not open it and do not click on any attachments.
- Protect your computer with security software.
- Make sure that your anti-virus software is up to date

- Never follow the messages from anti-virus software you encounter whilst on the internet. Only follow the anti-virus instructions from the software you have installed on your computer.
- Always use a firewall. This is the primary method for keeping a computer secure from intruders and provides users with secure access to the Internet. Basically it is a piece of software that sits between your computer and the internet, protecting the computer from incoming attack from hackers or viruses.
- Ensure that your software is up to date. For example, Windows software is routinely updated on the second Tuesday of each month (security updates are issued on that date). Should a critical update be necessary between monthly updates, make sure it is installed immediately. It only takes a few minutes to download and install - *it takes much longer to recover from a cyber hack.*
- Windows updates for Windows Defender, the built-in security system, can be installed automatically and actually are in Windows 10.
- Use strong passwords (e.g. use a mixture of letters and numbers – upper and lower case). Keep your password safe and change it regularly. Don't use the same password for every account you use online. Weak passwords can allow hackers to use victims' email to gain access to many of their personal accounts, leaving them vulnerable to identity theft and fraud.
- Protect your personal information.
- Review bank and credit card statements regularly.

If you become the victim of cybercrime or receive a potential scam email or text, this can be reported to Action Fraud, National Fraud Intelligence Bureau – tele 0300 123 2040 or at the website link **http://www.actionfraud.police.uk/report_fraud**

In Wetherby U3A, we take data protection very seriously.
Please ensure you take steps to protect yourself!

U3A members who can help with computer security advice:

Mike Green – Telephone 01937 582810 email: chairu3awetherby@gmail.com

Brian Taylor – Telephone 01937 586694 email: btu3awetherby@gmail.com

Some useful websites:

http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/online-threats-to-consumers

https://www.gov.uk/topic/dealing-with-hmrc/phishing-scams

http://www.actionfraud.police.uk/scam-emails

https://www.cyberaware.gov.uk/

https://uk.norton.com/cybercrime-prevention