Email and Security

U3A Radlett Computer Group Meeting

6-Oct-2014

V1.1

Agenda

- Introduction
- Email
- Security
- Q&A

U3A
THE UNIVERSITY OF THE THIRD AGE

Introduction – Gary Harding
eMail:- U3A@GaryHarding.com

Spent more than 40 years working in the IT industry

At one time worked as a security consultation for a large IT company but has not been my main role for many years

I continue to have an interest in computers and security

I often talk too quickly and sometime too quietly!!

- If you can't hear or understand me do ask – I will not be offended!
- Feel free to ask questions as we go but I may delay the answer to later in the presentation or to the Q&A section at the end

U3A
THE UNIVERSITY OF THE THIRD AGE

Things to remember

- A lot of what I say today may sound scary or put you off using your computer but please don't worry too much – some basic common sense and a little bit of knowledge will generally keep you safe (but there are no guarantees!)
- As with most thinks in life if something sounds too good to be true it probably is bad for you. No one is going to give you free money, make your life a lot better or sell you something for considerably less than it is worth. These are almost always tricks to get you to disclose information which can cost you considerably more than you might have gained.

U3A
THE UNIVERSITY OF THE THIRD AGE

Email - history

- Email has been around ever since there was shared use of computers
- Originally it allowed people that used the same computer to pass messages to each other and grew dramatically when computers started to be networked to each other and further once these networks were expanded to link to personal home computers
- It is a great way of providing asynchronous (i.e. not at the same time) communication and keeping in touch with people
- It has become the ‘vector’ for many of the security problems

U3A
THE UNIVERSITY OF THE THIRD AGE

Email – things to consider

- Your eMail address is like your postal address – people need it to send you information (bills, letters, magazines) but once someone has it they can also send you things you don't want (Junk Mail / Spam) or pass it on to other people / organisations to do this
- Email is more like a postcard than a letter – anyone that gets to capture the internet traffic can read it. Don't put anything in an eMail you would not be willing to let anyone/everyone see.

U3A
THE UNIVERSITY OF THE THIRD AGE

Email – things to consider

- Use bcc when sending messages to a lot of people – this will prevent everyone who gets your eMail seeing everyone else's eMail address (latest U3A newsletter has more on this).
- Email addresses are free and easy to create (e.g. Gmail, Yahoo, Outlook.com). Consider having more than one eMail address, e.g. one that you only use for family and friends and another one that you use for newsletters, website subscriptions, etc.
- If you really need to send a 'secret' eMail use some form of encryption (but can be complicated / difficult).

U3A
THE UNIVERSITY OF THE THIRD AGE

Email - spam

- Spam is any unwanted eMail
- Frequently can be identified by misspellings, bad English and use of odd characters (e.g. 0 – zero instead of O ‘oho’, 1 – one instead of l, etc.)
- Often trying to sell you something but can be more malicious
- Most email systems (e.g. Hotmail, yahoo, gmail, Outlook and AOL) have filters that try to separate spam from real eMail but these are not 100% perfect (some spam will get into your inbox, some real eMail will get treated as spam)
- There are some services (e.g. Spam Arrest, Spamfighter) that require pro-active approval but can make eMail slower or prevent good eMails getting through and are not generally recommended

U3A
THE UNIVERSITY OF THE THIRD AGE

Email - spam

- Avoid opening spam email – e.g. pictures which may open automatically – or clicking on any links, as these can be used to tell the sender that they have reached a real person who might be interested in the subject and will just get you more spam
- Don’t reply or click on any ‘unsubscribe’ links in an eMail – again they just confirm to the sender they have found someone
- Don’t buy anything from a spam email (more on this later)
- Don’t forward ‘chain letters’, even if they appear to be a warning or reasonable appeal, this is just turning you into a spam sender

U3A
THE UNIVERSITY OF THE THIRD AGE

Email – Viruses and Trojans

- These are typically programmes than run on your computer that do one or more of:
  - Gather information about you that can be used to impersonate you or get access to your finances
  - Stop your computer working (or slow it down) sometimes ‘just for fun’ but more recently to block access to your computer and demand money for it to be unlocked
  - Work with other computers to disrupt other people’s / companies computers (‘botnets’)

U3A
THE UNIVERSITY OF THE THIRD AGE

Email – Viruses and Trojans – how do you get / avoid them

- The most common way to get them is to open a malicious attachment from an eMail or download them from a web site but sometimes it can be from just going to a specially constructed website
- Unless you are absolutely certain that the attachment is from someone you know (more on this later) and you are expecting it – do not open any attachments that you get sent in an eMail. Most commonly the problems are with .exe files but you can get them from word processing, spreadsheets and even pdf files
- Run a good Anti-Virus programme – these tend to be operating system specific but there are many good ones available (Norton, Kaspersky, AVG, AVAST) – some are free or have free versions and some banks (e.g. Barclays for Kaspersky) will give you a free licence for them

U3A
THE UNIVERSITY OF THE THIRD AGE

Email – phishing / vphishing

- An attempt to get you to disclose importation information about yourself (typically financial details but may also be passwords) in order to get access to your money or other private information. Often appear to be from a bank, someone offering you money or a ‘friend in need’.
- “Phishing attacks are by far the most popular form of cybercrime in the 21st century. Phishing scams increase in quality and quantity every day. Whereas spam tends to be merely an annoying distraction, phishing frequently leads to real financial losses”
- Can appear as a threat (e.g. if you don’t reply your account will be closed, eMail blocked, you will miss notifications, etc.)

U3A
THE UNIVERSITY OF THE THIRD AGE

Email – phishing / vphishing - how to avoid it

- Do not give out your financial information to anyone in an email, over the phone or on the internet unless you are 100% certain about them (they are reputable, you have used them before and if using a browser it has the ‘padlock’ symbol displayed)
- Try to use a different credit card for online purchases than you do for your normal purchases so you can spot unexpected items quickly. Using an account that you can check online (or will send you alerts about payments) means you can spot problems quickly and not have to wait for a statement

U3A
THE UNIVERSITY OF THE THIRD AGE

Email – phishing / vphishing - how to avoid it

- Use services like Paypal which put a barrier between your financial information and the seller
- Go directly to the site by typing in the address yourself and not via a link or search result
- Lookout for sites which offer to do things for you (e.g. apply for a driving licence, passport or submit a tax return) as these often take money for a service you can do freely or at a lower cost yourself (as well as the risk of exposing your information)

U3A
THE UNIVERSITY OF THE THIRD AGE

Email – impersonation

- It is reasonably easy to impersonate someone (or some organisation) in an eMail. Just because an eMail says it is from someone does not mean that it is!
- Look at the address after the name – if the two don't match, e.g. it claims to be from your bank, facebook, your ISP or eMail provider, but the eMail address looks wrong or ends in, for example, .ru (for Russia), it is probably not from them!
- Check links by hovering your mouse over them before clicking – most browsers will show the actual web address you will go to - if it looks odd or wrong it probably will take you to someone else

U3A
THE UNIVERSITY OF THE THIRD AGE

Email – impersonation

- If an eMail appears to be from someone you know but asking you something odd (e.g. to send them money, give them a password) contact them by another route, e.g. by phone or text message, and check that it is for real (it probably isn't)

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – introduction

- CIA – Confidentiality, Integrity, Availability
- Confidentiality – keep the information I don't want others to know to myself
- Integrity – make sure that the information I have has not been corrupted
- Availability – make sure the information I have is available when I want it

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Availability

- Backup, BACKUP, BACKUP your data!
- Despite all of the things we have discussed there is still a chance that your systems and data might become unavailable from a virus, damage (e.g. fire or water), mechanical failure, theft, etc.
- Backup everything that you do not want to lose or would be difficult to recreate. E.g. photos, documents, spreadsheets you have created, applications you have bought.
- Back it up regularly, no point in just doing a backup once a year – you might lose a lot of things you wanted to keep

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Availability

- Backup in more than one place. There is no point in just having a backup on a 2nd drive attached to your computer – you can lose both of them at the same time.
- A local backup is useful for fast recovery from accidental deletion, etc.
- Backup to a memory stick, USB drive, DVD disk and move it elsewhere (one of your children's or friend's houses?).
- Use online backup (One Drive, Google Drive, iCloud, etc.)
- Use a combination solution (e.g. CrashPlan)

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Confidentiality - Hotspots / Cyber Cafés

- Wi Fi hotspots are a common and useful way to get online, particularly if you are abroad
- Generally most Public Wi-Fi hotspots are not secure!
- Unless your data is encrypted the person that controls a hotspot can easily monitor all of the traffic that goes through it. E.g. this can include your passwords, account and credit card details, contact lists, etc.
- Cyber Cafes are similar – whoever runs the computers controls the programmes that are on them and can monitor what you are doing

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Confidentiality - Hotspots / Cyber Cafés – can I use them?

- If you are using an unknown / unusual hotspot or cyber café be careful about what you type in and avoid typing in passwords, particularly ones for eMail accounts and financial institutions
- Do not enter any personal data into a hotspot login screen to get access (recent example quoted on Radio 4 was of people entering their date of birth, name of first child, etc., all of which could help someone to impersonate you)
- Using the banking application provided by a financial organisation is normally OK as they should have ensured that the data is encrypted before it leaves your device

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Confidentiality - Hotspots / Cyber Cafés – can I use them?

- Use eMail accounts that allow 2 step verification (e.g. Gmail and Outlook.com) – this means that even if someone gets your password they still can't access your account
- You can generally trust libraries and other well known organisations a bit more than a random hotspot but still be careful – if they are not properly managed the person that used it before you may have left some tracking software running on it
- For your own Wi Fi hotspot (e.g. wireless router) make sure it is encrypted (WPA / WPA2) and consider turning off WPS

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Passwords the problem

- Passwords (like PINs) are the bane of the internet
- Many sites request them to ‘protect’ your information and say you should not write them down, use the same password for more than one site and change them regularly
- They may also require rules to be met (upper and lower case, length, include numbers & symbols, etc.)
- This is impossible for most people who may have 10s, 100s or even more sites they access that request passwords
- However not following the rules does make you vulnerable

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Passwords the solutions?

- Biometric information (e.g. fingerprints) is starting to be used but not perfect and needs much more research and development
- Classify the type of site you are using and use passwords appropriate to each
  - Simple password for sites which have no confidential information
  - More complex password for sites that you would prefer not to be exposed but would not cause much of a problem if they were
  - Very complex passwords that you change and keep separate for financial and other key sites

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Passwords the solutions?

- To avoid writing passwords down use rules that are easy to remember (e.g. first grandchild's name and year of birth / age)
- If you need to write them down to remember the rules you have used keep them in an password protected / encrypted file and not on paper on or near your computer / device
- Use a trusted password manager (e.g. Lastpass) but use a strong password and multifactor authentication for them (but remember the danger of keeping 'all your eggs in one basket')

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Encryption - history

- Has been around since roman time (Caesar Cypher) and probably earlier
- Often thought of as the remit of spies
- Now used everyday on the internet (the ‘padlock’ symbol you may see on your browsers shows that the data being passed between your computer and that site is encrypted)
- Makes it very hard for your information to be exposed but not impossible (you may have heard of the ‘Heartbleed’ bug recently)

U3A
THE UNIVERSITY OF THE THIRD AGE

Security – Encryption

- If you want to keep your information secure encrypt it (but you probably will still need to have a password or PIN)
  - Winzip and 7Zip can encrypt files
  - Bitlocker (Windows) can encrypt a disk
  - PGP can encrypt eMails and other items, can also provide integrity checks
- Unencrypted versions of the data may still be around (on backups or temporary files)
- If you lose the password to some encrypted data it is very unlikely that you will ever be able to recover it!

U3A
THE UNIVERSITY OF THE THIRD AGE

Q & A

The End