This guide is intended to help Ffriends feel secure about their use of personal computers, tablet computers and smart phones. It is based on a very informative Guide issued by AgeUK which is a free download (click here)and covers the subject in greater depth.
For many people the internet has made life easier and is an excellent source of information but it needs to be used wisely. You already have a lot of the skills and intuition to stay safe online. All you have to do is apply the same common sense you use in everyday life. For example, you wouldn't open your front door and invite a stranger into your home, so it makes sense not to open email attachments from someone you don't know and you wouldn't give your front door key to a stranger either.

GDPR data security -

The General Data Protection Regulation came into force in May 2018 and introduces checks and balances on how personal data is stored and used. The Area Meeting Data Protection Officer and the Membership Clerk comply with the regulations but Ffriends need to be aware that they may hold data that is also covered. This may be data relating to their Local Meeting Friends or email lists for the purpose of sending Newsletters etc.
Whilst it is acceptable for Friends to hold this data they must be aware of their responsibilities in terms of security and accuracy.
The GDPR requires organisations handling personal data to do so according to its six data processing principles, namely that:
a) it is processed fairly, lawfully and transparently
b) it is collected and processed for specific reasons and stored for specific periods of time, and that it is not used for reasons beyond its original purpose
c) only the data necessary for the purpose it is intended is collected, and not more
d) it is accurate and that reasonable steps are taken to ensure it remains accurate
e) it is kept in a form that allows individuals to be identified only as long as is necessary
f) it is kept securely and protected from unlawful access, accidental loss or damage
There is a very detailed Guide to the GDPR available (click here).

Friends who do hold such data as may be covered by the regulations should pay careful consideration to the security of their computers. Data should be kept on pen drives and only connected to the system when it is required. The data subjects must be made aware of how their details can be amended or deleted and emails relating to requests for changes should be kept.
The Area Meeting Data Protection policy is available on the Area Meeting website - http://smquakers.org.uk/downloads/dpp2018.pdf
If you require further guidance please contact the Data Protection Officer whose details are in the List of Friends.

Being aware of the risks that come with using the internet and taking steps to avoid them means you can enjoy the internet safely.

Personal data security -

Email encounters

Your email accounts are usually protected so that suspicious emails are blocked out without you having to do anything. However, it's still important to be aware of the common types of email scams so that you can protect your personal information.

Spam

Common types of spam include:

- advertisements from a company
- an email telling you about a scheme to make you rich
- an email warning you of a virus
- an email encouraging you to send the email onto more people.

These may even come from an email address that you recognise, such as a friend or family member, as sometimes accounts can be hacked into and fake emails sent out to all of that person's contacts.

Phishing

Common types of phishing scams can be:

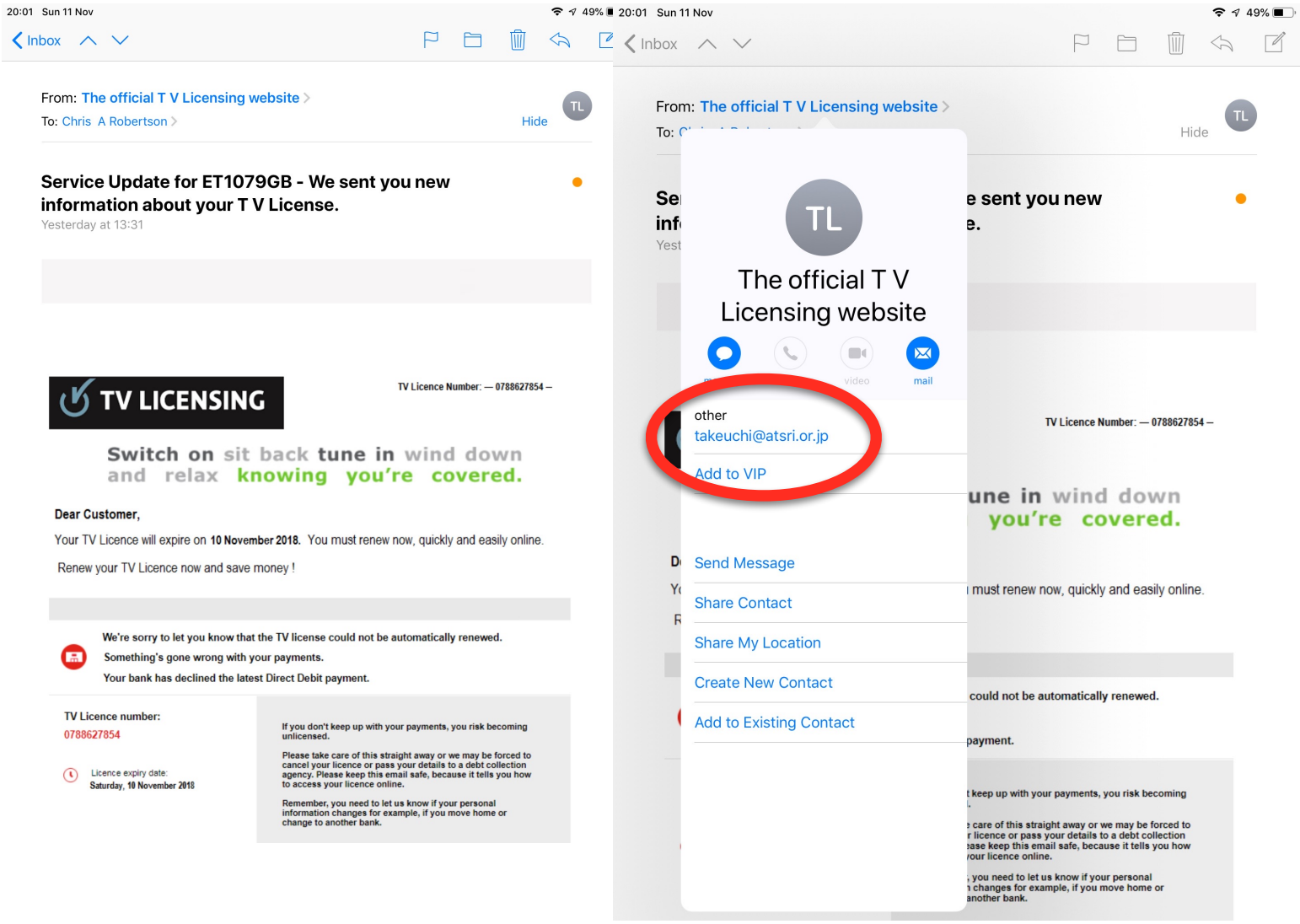
- from your 'bank' asking you to update your security information (e.g. your password) or your account will be closed
- from a well-known company (e.g. PayPal, Amazon) asking you to update your account details or install a programme on your device
- from a government agency (e.g. HMRC) telling you about a rebate or penalty
- an email saying you have won some kind of prize, lottery or inherited a large amount of money

- an email supposedly by someone you know asking for money because they are stranded somewhere or need medical assistance
- an email with a link or document attached for you to click on or open. If you click on the link or document, a virus may be released onto your device so fraudsters can get access to your personal information.

How to recognise spam and phishing emails

The sender's email address may look official but it is not the actual email address of the bank or company. Always check with your bank if you are unsure.
The email may have errors in its spelling or grammar, or be written in an unusual style.
The email does not use your proper name, but instead starts with a general greeting like 'Dear customer'.
There's a sense of urgency, for example threatening that unless you act immediately, your account will be closed or a deal will expire.
It may contain a link to a website that looks very similar to the company's real one but is actually a fake site asking for your personal details.
There may be a request for personal information, such as your username, password or bank details.
There may be a request for money, for example for processing your prize, or for helping someone in need.
There may be a document or link to open and either no message or some short text saying 'Check this out' or 'See what I found' without further explanation.

This is an example of a typical phishing email. It appears to come from a legitimate source. But by clicking on the sender's email address it is clear that it is not from TV Licensing.



What to do if you receive a suspicious email

- **If in doubt delete it without opening it.** Do not open emails from strangers or emails that you suspect may be a scam.
- Do not open an email link or document attachment unless you are sure it's safe.
- Do not reply to spam or suspicious emails as this demonstrates that your email address is active so they may contact you again.
- Banks and other financial institutions never ask for personal information in an email. If you receive a suspicious email claiming to be from your bank, contact your bank directly by phoning them or typing their web address into your browser (not by following the link in the email).
- If it's about account information, phone the organisation directly to ask about the email, using the phone number found on their official website.
- Don't panic if you get an email that has a sense of urgency and threatens to close your account. Take your time to check the details first before reacting.
- If you receive a strange email from a friend or family member, send them a separate email or call them to ask if it's genuine.

Computer scams

Beware of a common scam. The fraudsters phone you claiming to be from a well-known IT (information technology) firm, asking you to follow a few simple instructions to get rid of a virus, update your software or fix another issue with your computer. If you do as they ask, they will upload software called spyware onto your computer, which allows them to access any personal details you have stored on your computer. Legitimate IT companies never contact customers in this way. Never respond to a phone call from someone claiming that your computer has a virus. If you get a call like this, hang up straight away.
There are also recorded message calls claiming that your internet connection is about to be disconnected and asking you to return the call - just hang up, don't call back and ignore the message.

Passwords

Avoid weak passwords **-** Weak passwords are made up of common sets of letters or numbers.
Use a complex set of upper/lower case letters and symbols. If you find it difficult to remember passwords consider using a Password Manager - there is a review of password managers here - https://uk.pcmag.com/password-managers/4296/the-best-password-managers
Some internet browsers have built-in password managers. This is a tool that remembers your passwords for different sites and fills them in for you automatically.
When you log in to a website for the first time, the password manager will ask if you want it to remember the password. You have the choice if you want it to or not. It can save time to use this function, but it will only work on your own computer. Make sure that your computer is only used by people you trust.
If passwords with numbers and symbols are too hard to remember, using three random words together can make a stronger password, as long as those words don't contain your personal information.

Choose different passwords

Use different passwords for different websites or accounts. Using one password for all accounts is a potential security risk because if a stranger gets access to (or hacks) your account on one site, they will be able to log in to all the accounts that share that password.

Be careful writing down your passwords

Never write down your password. If you need a written reminder, try to write a hint that only you'll understand, rather than the actual and complete password itself. If you do write anything down, keep that information somewhere safe away from your computer.

Online shopping and banking

If you make purchases or bank online, make sure you protect your financial information. Use a website that's secure when entering card information.
How to spot a secure website

- The website address should begin with 'https://'. The 's' stands for 'secure'.
- If the address bar is green, this is an additional sign that you're using a safe website.
- Look for a padlock symbol in the browser next to the website address. Don't be fooled by a padlock that appears on the webpage itself.

- Websites that offer secure payments and other financial transactions, such as banking, need a security certificate. To view it, click on the padlock symbol to check that the seller is who they say they are.

Tips for shopping and banking online safely

- You'll never be asked for your card PIN (personal identification number) but you may be asked to provide the security number for your debit or credit card, referred to as 'CVV', 'CVC' or 'CVV2' (Card Verification Value).
- If you get a pop-up message warning you about a website's security certificate, be very cautious. If you continue, you may be redirected to a fake website, designed to let somebody else read the information you are sending, such as log-in details.
- Use online retailers that have a good reputation, either as high-street shops or as established online stores.
- If a deal looks too good to be true, it probably is. You could do an internet search to see whether anyone else has had problems or if it's a well-known scam.
- Always use a credit card for internet transactions, or check to see if your debit card provider offers any protection. If your purchase costs more than £100 and you use a credit card, the seller and your card company are equally responsible if anything goes wrong.
- After you've finished using a secure site always make sure you log out.

Social networking

Social networking websites are online communities where you can connect with people who share your interests.

Social networking sites can be targets for people who want to steal personal information, but it's easy to stay safe by following a few sensible guidelines.

- Be aware of who can see your profile. Most social networks allow you to choose who can see your profile and how much they can see, but you may have to change your settings to make it private.
- Be wary of publishing any information that identifies you, such as your phone number, photos of your home, your address, date of birth or full name.
- If possible, pick a username that doesn't include any personal information. For example, avoid using 'annajones1947'.
- Set up a separate email account that doesn't use your real name to register with the site.
- Use a strong password that is different from the passwords you use for other accounts.
- Be cautious with people you've just met online who ask you to reveal personal information or who want to meet you very quickly.
- Be on your guard against phishing scams.

Protect your computer

Protecting your computer from harmful malware or viruses is simple, just follow the tips below.

Install anti-virus software

Viruses are malicious programs that can spread from one computer to another by email or through websites.

Anti-virus software helps to find, stop and remove these malicious viruses.

Install anti-spyware software

Spyware is an unwanted program that runs on your computer.

Installing anti-spyware software helps to protect your computer from these threats.

You can buy a complete package that includes everything you need, or get effective free software such as AVG (http://free. avg.com) or Avast (www.avast.com).

Online threats change constantly so once your software is installed, keep it up to date when prompted. This ensures that you have the highest level of protection.

Keep your operating system updated

The operating system is the main software program on your computer, which manages all the other programs on it – the most common systems are Microsoft Windows and Mac OS. Whichever operating system you have, keep it updated as this will give you better protection.

Protect your wireless network
If you use wireless internet at home, you will have a wireless router. You need to protect your wireless network (also known as wi-fi) so that people living nearby can't access it. Read the instructions that come with your router to find out how to set up a 'key' – a type of password – so that no one else can access the internet through your router.

Protect your tablet and your mobile phone
Tablets (e.g. iPad) and smartphones can now be used to do things like check emails, shop and bank online or explore the internet.
Tablets and smartphones need protecting just like computers do. Just like on computers, viruses on your tablet or smartphone could be used to get your personal details, slow your device down or spread viruses to other tablets or computers.
You can download anti-virus and anti-spyware protection for tablets and phones. A lot of good anti-virus protection for phones and tablets is free and can be downloaded online.
Some highly rated anti-virus apps, which are free, are:

- Avast mobile security (visit www.avast.com)
- Kaspersky internet security (visit www.kaspersky.co.uk)
- Norton mobile security (visit uk.norton.com/ norton-mobile-security)

These apps work on phones and tablets that use Windows, Android and Apple products.

Download the latest software and app updates
Your tablet or mobile phone may prompt you when there is a new software or app update. This will give your device the latest security protection and may provide some new features.

Password protect your device
You should also password-protect your phone or tablet, to make sure that only you, or people you trust, can use it. Password access is easy to set up, just follow the instructions that come with your device.

Being aware of the risks that come with using the internet and taking steps to avoid them means you can enjoy the internet safely.