Tackling Fraud Together – March 2018

A monthly bulletin providing the latest fraud alert information and advice

Knowledge Bank: Viruses & Spyware

Source: Get Safe Online www.getsafeonline.org

A virus is a file written with the sole intention of doing harm, or for criminal activity. Viruses and spyware are also known as 'malware'.

A Trojan is a program that appears harmless but hides malicious functions. Viruses may harm a computer system's performance or data. Some are noticeable to the computer user, but many run in the background, unnoticed by the user.

Spyware is a type of virus that is specifically designed to steal information about your activity on your computer. Spyware writers have a number of different objectives, mainly fraudulent financial gain. Spyware can perform a number of illicit functions, from creating pop up advertisements to stealing your bank login details by taking screen shots of the sites you visit and even logging the keys you type.

Potentially, a virus could arrive on your computer in the form of a Trojan, it could replicate itself before moving on to another computer (a worm) and also be designed as a piece of spyware. Viruses and spyware are types of malware, which also includes rootkits, dishonest adware and scareware.

The Risks

Viruses and spyware can attack your computer via the following means:
- Opening infected email attachments such as .exe files.
- Opening infected files from web-based digital file delivery companies (for example Hightail - formerly called YouSendIt, and Dropbox).
- Visiting corrupt websites.
- Via the internet, undetected by the user (worms are an example of this).
- Macros in application documents (word processing, spreadsheets etc).
- USB connected devices (eg memory sticks, external hard drives, MP3 players).
- CDs/DVDs.

Viruses and spyware can cause very serious consequences including:
- Identity theft.
- Fraud.
- Deletion, theft and corruption of data.
- A slow or unusable computer.

Internet security (antivirus/antispyware) software

It is vital to keep your internet security software up to date in order to provide the most complete protection. Thousands of new viruses are detected every day, to say nothing of the variants of new and existing ones. Each has a set of characteristics that enable internet security software manufacturers to detect them and produce suitable updates.

Most internet security software automatically downloads these updates (sometimes referred to as 'definitions') on a regular basis, as long as you are online and have paid your annual subscription (for a paid-for product). This should ensure protection against even the latest virus threats.

Internet security software scans for viruses in a number of different ways:
• It scans incoming emails for attached viruses.
• It monitors files as they are opened or created to make sure they are not infected.
• It performs periodic scans of the files on your computer.

Some internet security software also scans USB connected devices (eg memory sticks, external hard drives, MP3 players), as they are connecting. Some also highlights suspect websites.

Internet security software **will not** protect you against:
• Spam.
• Any kind of fraud or criminal activity online not initiated by a virus.
• A hacker trying to break into your computer over the internet.

It is not effective if it is switched off or not updated with the latest virus signatures, and do bear in mind that no internet security software is infallible, so a new strain of malware from a fraudulent attachment or bogus website may still evade your software.

Choosing internet security software

For personal and home office use there are a number of choices that you can take to decide which internet security software to buy. Whichever you choose, make sure it is a reputable brand from a mainstream supplier, and get the best you can afford. Here are a few of the best-known suppliers, but please note we are not recommending one over the others: Norton, Kaspersky, McAfee, Bullguard, Sophos, AVG, Avast, Bitdefender

Some manufacturers and retailers provide various security software bundled with the computer. You do not have to use the security software supplied, but if you decide to keep it, do not forget to subscribe once the free trial period is over so that it stays up to date.

Where to get internet security software

Antivirus/antispyware software and internet security packages are available to purchase from a variety of high street and online retailers as well as from the software manufacturers' own websites. When purchasing in store, it is normal to load a disk and then download updates over the internet when prompted. When purchasing online, you will automatically download the latest version incorporating all updates.

Free antivirus/antispyware software and internet security packages, are also available from some internet service providers (ISPs) and banks. It is also possible to download free software from the internet, but be sure you are using a trustworthy website.

Prevention is better than cure

Apart from installing internet security software and keeping it updated, we recommend a number of other ways in which to keep your computer protected against viruses and spyware. After all, prevention is better than cure.
• Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
• Uninstall one antivirus program before you install another.
• Be careful with USB connected devices (eg memory sticks, external hard drives, MP3 players) as they are very common carriers of viruses.
• Be careful with CDs/DVDs as they can also contain viruses.
• Do not open any files from web-based digital file delivery companies (eg YouSendIt, Dropbox) that have been uploaded from an unknown, suspicious or untrustworthy source.
• Switch on macro protection in Microsoft Office applications like Word and Excel.
• Buy only reputable software from reputable companies.
• When downloading free software, do so with extreme caution.

How to report scam mail

Source: Royal Mail

Like telephone, email and online scams, there are a few different types of scams that can be sent in the post. Sometimes they are tricky to spot. Royal Mail want to help you look out for scam mail, and explain how you can avoid falling victim to it.

What is scam mail?

Scam mail can take the form of fake lotteries and prize draws, get-rich-quick schemes, bogus health cures, investment scams and pyramid schemes. Sometimes these can be sent to you if a scammer has got hold of your contact details fraudulently.

N.B. There's a difference between scam mail and legitimate mail sent by companies to promote lawful services or genuine goods. Scam mail is sent for the sole intention of obtaining money through deception and/or fraud. We want to know about potentially fraudulent mail. We can then work with the relevant authorities who can investigate and take action.

What to do if you think you've received scam mail

If you think you or a family member is receiving scam mail, please complete a Scam Mail Report and send it to:
FREEPOST SCAM MAIL
Or you can email: scam.mail@royalmail.com, or phone: 03456 113 413 (message service only)

Please include any items of mail you've received that you believe were sent by fraudsters. This should include the original envelope it was sent in.

Other ways to report mail fraud:
You can contact Citizens Advice consumer service by:
•calling 03454 04 05 06
•writing to Citizens Advice consumer service, 2nd Floor, Fairfax House, Merrion Street, Leeds, LS2 8JU

How you can help avoid scam mail
If you're moving home, Action Fraud recommends using a 'Redirection' to reduce the risk of identity fraud. They recommend redirecting mail from your old address to your new address for at least a year.
If you hold power of attorney for somebody, you can apply for a Redirection on their behalf. You can do this if you believe they're a victim, or are vulnerable to being a victim, of scam mail.

Spam Text Messages

Source: Get Safe Online

Unsolicited texts from people you don't know are at best annoying, and at worst can contain links to malicious websites designed to steal your personal details and, ultimately, defraud you. Spam texts trying to persuade you to contact the sender regarding an accident claim, PPI claim, free holiday or car, a medical remedy or similar are not only tiresome ... they are illegal.

Authentic text messages should include the name and contact details of the sender. You should have given consent for them to be sent, but you may have forgotten, or not have realised.

If you receive a spam text, do not reply or forward it, but delete it.

You can also report spam texts directly to your mobile phone provider, all of whom have collaborated to set up a tool which collates all the information from the 7726* short code in real time. Dialling 7726 (or for Vodafone subscribers, 87726) enables your provider to take early action to block numbers that are generating spam on their networks, and report them to the regulators.

We recommend that you report spam text messages directly to your mobile phone provider free of charge by forwarding them to 7726 from the device they are received on.

'Which' also operates an online reporting service for scam texts and phone calls, here: www.which.co.uk/consumer-rights/advice/how-to-deal-with-spam-text-messages

*7726 are the corresponding numbers for S P A M on a phone keypad

How can I be sure that the collection leaflet or bag that has been posted through my door is legitimate?

Source: Textile Recycling Organisation

So how do you spot a bogus charity collector?

Unfortunately, there a number of clothing collectors who give the impression that they are collecting on behalf of a charitable or philanthropic cause, but they are actually purely commercial operations. Some will put out fake leaflets or bags which state the name of a legitimate charity or something very similar. In addition, some so called "Bogus Charities" put out leaflets/bags where they believe that there is going to be a legitimate charitable collection taking place. They then take the bags that have been put out for the legitimate charity collection and if caught they use the excuse that they thought that the bags had been put out for their collection.

There are a few simple things that you can do to check whether the collection leaflet or bag that you have received is for a genuine charitable collection. You can:

- ✓ Check to see if the collection purports to support a genuine UK registered charity (with the registration number given). This should not be confused with other numbers like "Company Numbers" or "Export Numbers" which have no relevance in this case.

- ✓ Check to see if the collection organiser is signed up to the Institute of Fundraising's Code of conduct or bears accepted kitemarks, such as the FRSB tick or the ACS/IOF membership logo. Any of these could indicate that the collection is a genuine charitable collection.

- ✓ Check to see whether the named collector is a member of the Textile Recycling Association. A full list of memberscan be found on the website. If the collectors are genuinely members of the Textile Recycling Association then this would be a strong indication that the collection has the correct licences in place and is legitimate.

- ✓ Check with the local authority to see whether the collection is licensed. With the exception of a few big national collection charities, most charitable door to door collectors are required to obtain a licence from the local authority in which they are operating.

- ✓ Contact the charity that the collection will supposedly benefit, as they should be able to tell you if a genuine collection is being done in your area or not.

The Charity Commission (www.charity-commission.gov.uk) provides further guidance on their website about how to ensure that you only donate to legitimate charity collections.

If you suspect that an unauthorised person has collected the clothing that you have put out, you can telephone your local police to report a theft. If you suspect that a bogus charity collection is taking place you can also contact the Action Fraud Helpline on 0300 123 2040. If you can remember which charity was meant to benefit you can also call the charity concerned.

FREE call blockers for vulnerable people

The National Trading Standards Scams team is working alongside trueCall to provide "trueCall Secure" units to people living with dementia or in vulnerable circumstances (i.e. living with a disability or health problem (either physical or mental), suffered a recent bereavement, been a victim of scams, or receiving scam phone calls).

If you are eligible for a free call blocker a unit will be sent directly to you. You will then receive a call from a qualified engineer to arrange a time for them to set up and install the unit, they also be able to will show you how to manage the units' settings. Once you receive a unit, it will become yours to keep and the NTS Scams Team will not be asking for it to be returned at any point. There is no cost to the user for the unit; however, we recommend that the "caller display" service is activated on the user's phone line for the unit to perform at its best.

One month after installation you will be contacted by a member of the NTS Scams Team and asked to complete a short survey to assess how effective the unit has been at blocking nuisance calls and how you feel about nuisance calls since receiving the unit.

To find out if you (or someone you know) is eligible for a free call blocker to be fitted, go to www.friendsagainstscams.org.uk

Recent News Articles

Leicester: Leicester tour company which sold pilgrimages to Mecca prosecuted for fraud

Scotland: Crime gang nets £7m from sophisticated phone scam

Royal Mail halts 3 million scam letters

Norfolk couple plead guilty to £17m fraud against pensioners

6 people jailed for running £37m 'copycat website' fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Sign up for free to Action Fraud Alert to receive direct, verified, accurate information about scams and fraud in your area by email, recorded voice and text message. http://www.actionfraud.police.uk/support-and-prevention/sign-up-to-action-fraud-alert