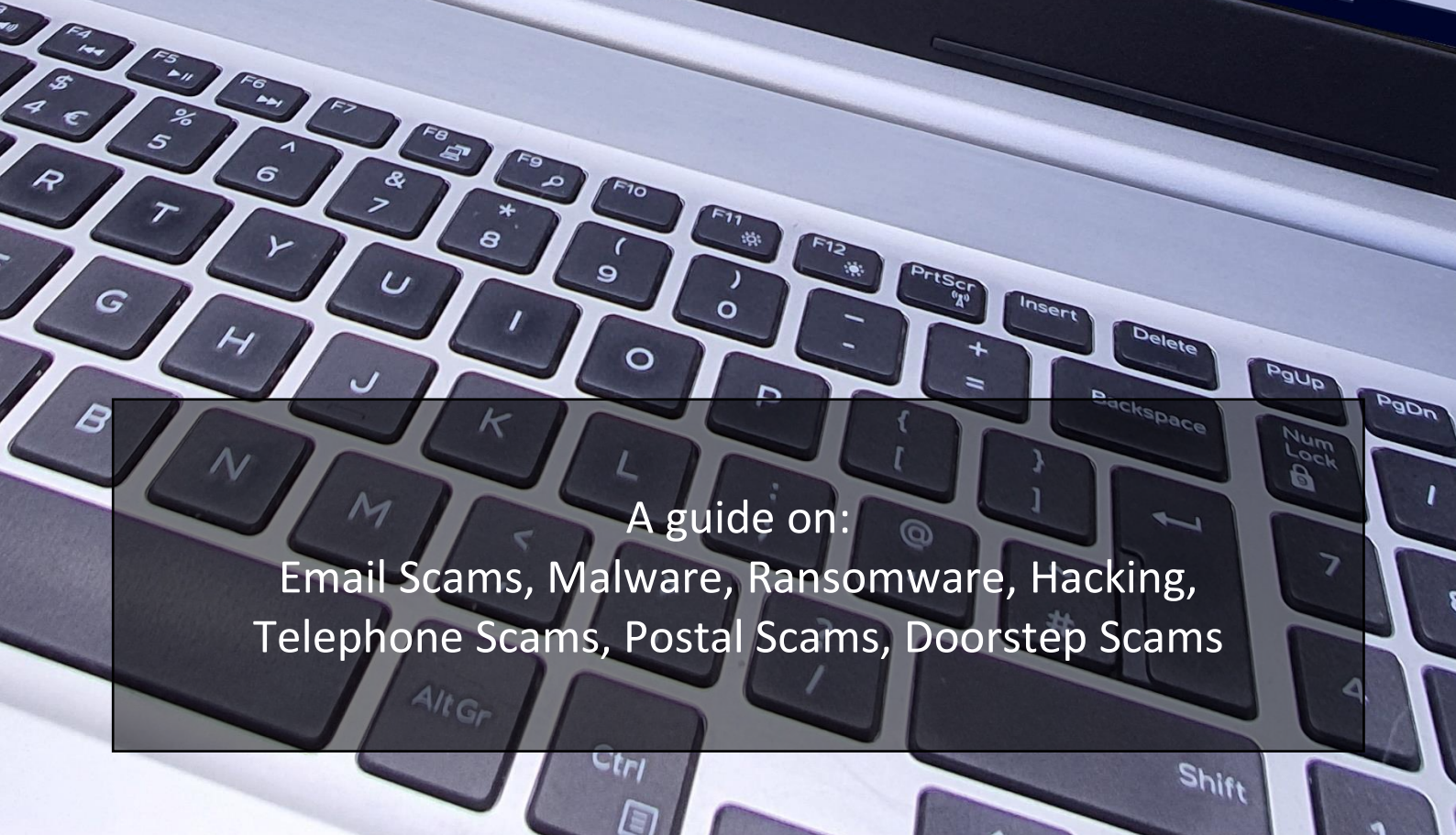




COVID-19 Advice/Support Guide: Cyber Security and Fraud Awareness



A guide on:
Email Scams, Malware, Ransomware, Hacking,
Telephone Scams, Postal Scams, Doorstep Scams

Cyber Security and Fraud Awareness

With the current coronavirus pandemic and people isolated at home, we are using our computers, netbooks/tablets, and smartphones a lot more to keep in touch. Sadly, there are individuals (and organised groups) that are exploiting the situation even more to rob you of your money or possessions. This guide has been produced to provide some tips on protecting yourselves against some of the many techniques in use today.

I have also added a couple of notes regarding telephone, postal and doorstep scams as we have also seen an increase in these techniques during these sad times.

What is Cyber Security?

The National Cyber Security Centre¹ states that:

Cyber security is the means by which individuals and organisations reduce the risk of being affected by cyber crime.

*Cyber security's core function is to protect the **devices** we all use (smartphones, laptops, tablets and computers), and the **services** we access online - both at home and work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of **personal information** we store on these devices, and online.*

Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine how we'd function without them. From online banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

What does that mean to me?

In plain terms, whenever you visit a website, open an email, click on a link through social media (e.g. Facebook, WhatsApp, Twitter, etc), there is a possibility that there may be hidden code that installs software onto your device, captures information stored on your device, or redirects you to unsafe websites where they will also try to access your personal data.

The Cyber Threat

There are so many ways a criminal will try to access your data or con you out of your finances, the main ones being:

- **Email Scams:** These include Spam emails, Phishing, spoofing, Spoofing, and Business/CEO fraud.
 - Spam Emails – these may not actually be malicious, but they are annoying at best. Spam emails are when you receive repetitive, unsolicited, or inappropriate emails that you have not signed up for. They are illegal in most countries.

¹ National Cyber Security Centre [online] *What Is Cyber Security*. Available from: <https://www.ncsc.gov.uk/section/information-for/individuals-families> [accessed 14 May 2020]

- Phishing – these emails ask you to click on a link, or open an attachment to the email, they are designed to access your personal information held on your computer, or by asking you to fill in personal details which will then be used in identity fraud.
- Spoofing – this is a method where an email header is altered to look like it has been sent by a genuine person or company. It may look as if it is from one of your own friends, or your own bank, shopping account (e.g. Amazon, eBay, etc). Thinking the email is from someone you know often means you will click on links or send information before finding out they were not genuine.
- Business/CEO fraud – this type of scam makes you think the email is from your own place of work, maybe your boss asking for information. More of a business threat but one to think about.
- **Malware** is software that can lock or destroy the information on your computer/device or cause damage in several ways such as:
 - Locking your computer, tablet, smartphone, etc, or making it unusable.
 - Capturing your personal data, deleting, or encrypting your data.
 - Using your own device to access other computers.
 - Accessing or using services that you will be charged for (e.g. international or premium rate phone calls).
- **Ransomware** is a form of malware, it prevents you accessing your computer, tablet, smartphone and asks for payment to have the device unlocked. Even if you did pay the ‘ransom’ it is possible that you will not get your system unlocked.
- **Hacking** is when an individual or organisation accesses someone else’s website, or accounts, and uses them to either access a network, accounts, spying on others, or as a challenge for those with hacking skills.
 - Website hacking – This is where an individual accesses your website using a logon and password, in most cases they will use software to logon multiple times using different passwords until the actual one has been found. Once into your website the individual (or organisation) can alter your website pages, add links to their own sites, or simply lock you out of your site to hold you to ransom.
 - Account hacking – This could be any account you access online, e.g. your bank, credit card, shopping, etc. Again, this will be an individual using your login details, either using guesswork or software that will log in multiple times until they have cracked your password.



Identifying the Threat

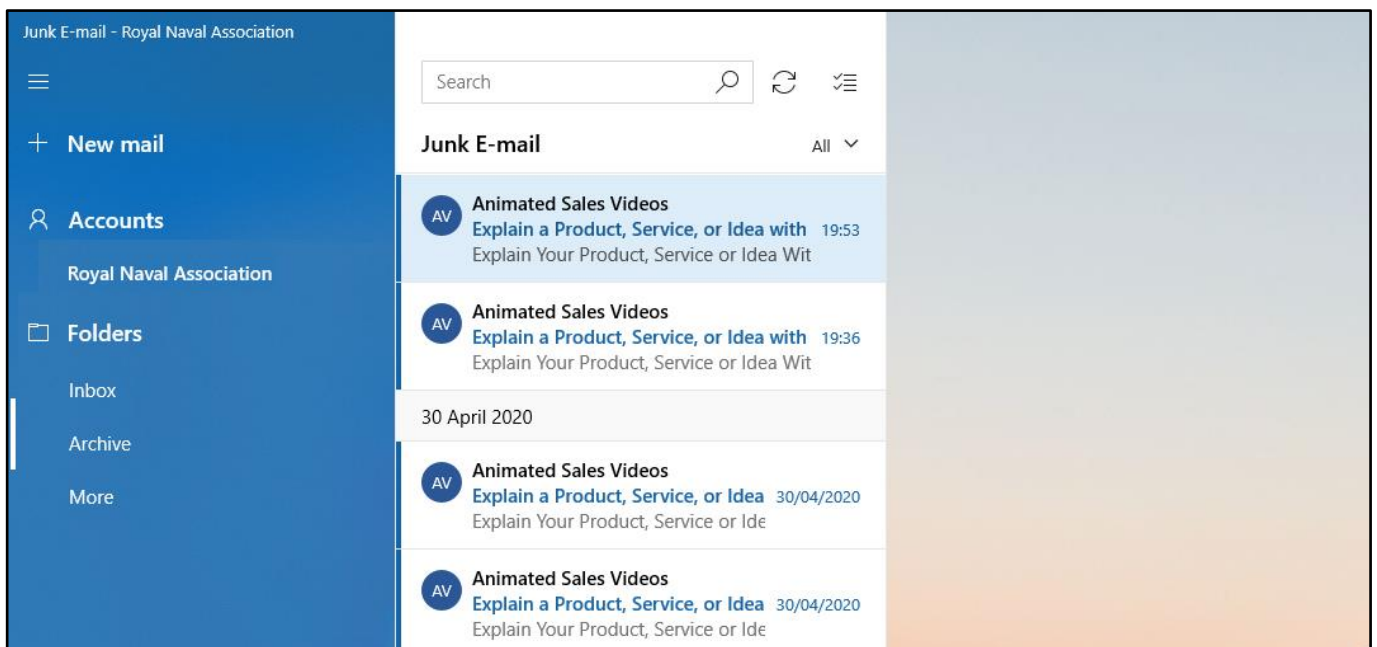
Now we know some of the threats to our computers, laptops, tablets, and smartphones we need to find a way to identify them to put safety measures in place. Thankfully, a lot of phishing attempts via email are so poorly worded that they are easy to spot. Sadly, this is not the case with the more serious criminals and are becoming increasingly harder to spot.

Email scams

Most emails sent worldwide today is unsolicited, junk mail sent out in bulk to a database of email addresses obtained legally or illegally. You may have seen websites asking you to create an account to use their services, once subscribed these lists can be hacked and/or sold onto others. Software can be used to seek out email addresses from the internet and compiles master lists for others to use. Other software simply generates email addresses, if you acknowledge these emails then the originator knows it is a valid address and will keep it in their database.

The type of email you will see in your inbox (or Junk Mail folder) include, but are not limited to the following:

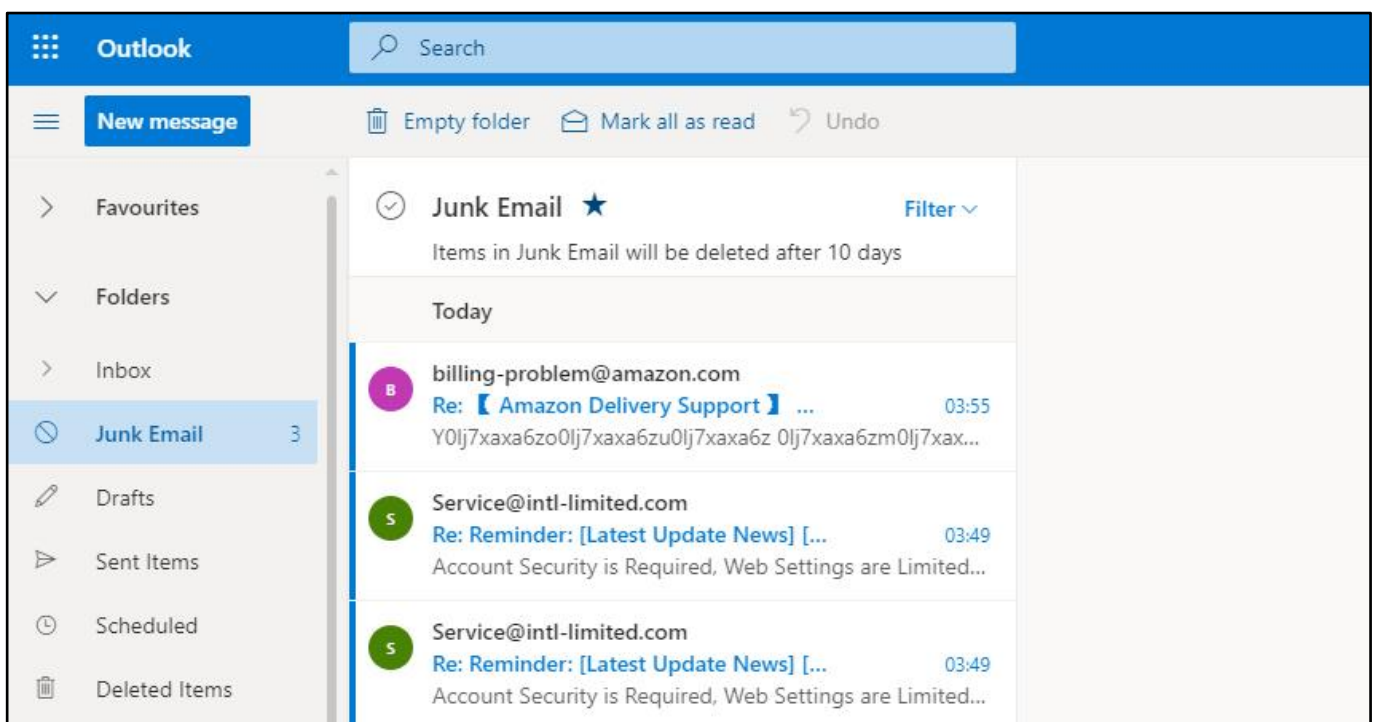
- Advertising online products or services (e.g. pharmacies, dating, gambling, etc).
- Charity appeals (e.g. at present there are several COVID-19 emails saying they are collecting for charity, not all will be genuine).
- Virus warnings to say you have been infected (often with a link or number to have the virus removed).
- Get rich quick emails (e.g. join this company and we will make you rich, or you have been left \$1million in a will).
- Chain emails asking you to forward the email on to others.



Spam emails

Some email scams have clear signs to look out for:

- It has been sent from someone you do not know (this could be a person or organisation, e.g. an email from a particular bank regarding your account, if you don't have an account with that bank then clearly this is a scam email (phishing/spoofing)).
- It appears to have been sent by a known company, but the email address does not match. For example, an email from 'Sky' about your account being on hold as a payment did not clear. The email address is skyaccount@TIYTvjbvc67.com this has not been sent from Sky, any links or attachments should not be clicked or downloaded. Always contact your service provider on a known number to verify if they had sent you any information relating to your account.
- The grammar and spelling may be poor (or intentionally misspelt to trick junk filters, e.g. 'p0rn' spelt with a zero so it does not get picked up by the keyword – spam/phishing/spoofing/CEO fraud).
- The offer is too good to be true -- and often is (spam/phishing).
- The urgency of the email (e.g. I need help immediately but cannot phone you now – phishing/spoofing).
- Contains a virus warning or attachments that you need to open or links to follow (spam/phishing/spoofing/CEO Fraud).
- The sender appears to be someone you know, but the subject line/wording does not match the way that person writes (e.g. 'OMG, please look at this video' – Spoofing), do your family/friends/colleagues really speak like this in an email?.



Phishing emails - accounts

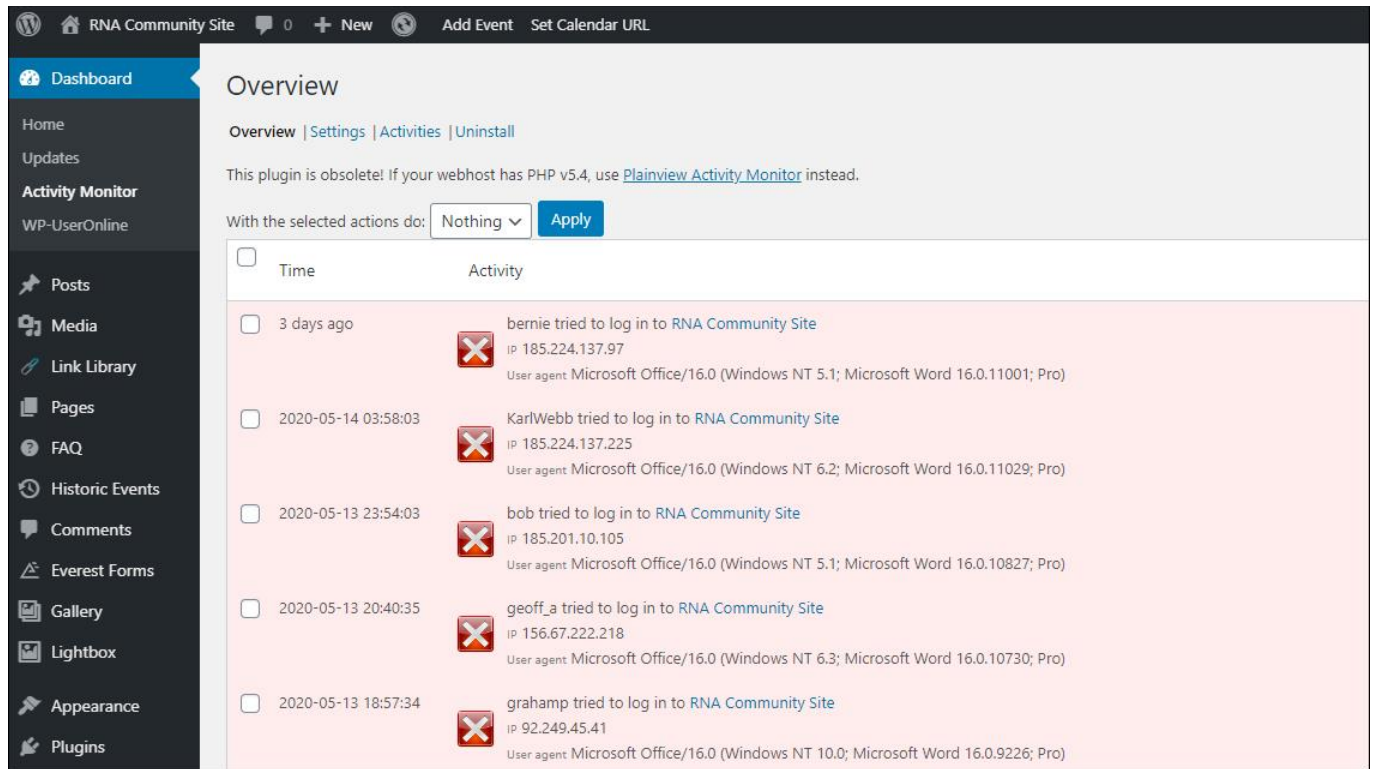
There are so many ways individuals or organisations will try to access your system, data, or finances via different website scams and hacks. Some involve a form of malware or social media scams:

- Grayware² – this is malware that does not actually cause physical damage but can be so annoying. Adware is the most common, we see adverts on social media pages, websites, and applications. This is often classed as ‘click-bait’ as it can lead you to a website where you will be asked to fill in a form or survey – this data can then be stored (and in some cases, illegally sold on to others).
- Social media downloads – one of my pet hates; several online videos or pictures can have embedded code that can install on your computer, laptop, netbook, smartphone. These are often posted onto social media platforms and users then forward them on to their family/friends/business colleagues. One example posted on the Norton security website related to the television show ‘Breaking Bad’, a link on Twitter stated that a leaked copy of the next (unaired) episode could be downloaded for free. The link took users to a page where the file was downloaded but also sent a link to another file needed to play the episode, this was an affiliate program which made the spammers money, but could have had far more serious consequences.
- Browser extension adware and malware – most browsers in use today can be tailored to individual needs with browser extensions. However, these can be used to steal your information as they track your site visits and usage, passwords, personal data, etc. Be very wary about downloading and installing browser extensions from sources you do not know.
- Ransomware – has been around for a long time on computers and laptops, they are now found on netbooks and smartphones as technology allows more files, photos, and documents to be encrypted. Ransomware is usually found when visiting infected sites (after clicking links or internet searches), the software is automatically downloaded to your computer devices or smartphone. Your files or system may then be infected and usually encrypted; a ransom is then demanded to unlock the system.
- Website hacking – this is a serious concern as the hackers will use legitimate websites (e.g. RNA Community Site, BBC News, Amazon, etc) to host links or files that contain malicious software that can access your personal data or encrypt your system. This is extremely dangerous as you tend to trust links and files on those known sites.
- Personal website accounts – as well as the host of a website being targeted, individual user accounts can also be targeted. In some cases this may not be as dangerous as user accounts often have different levels of access and ability to create pages, upload files, etc, but their accounts could still be used to post links to compromised websites or files.
- Social media accounts – as with personal website accounts, social media is the biggest threat to other users, if an account has been hacked, all sorts of links, photos, video, files, etc, can be posted to the social media platform. Your ‘friends’ then see the post and believe it is safe as it has come from you, they click or download and then they too become infected with the virus, malware or ransomware.

² Norton (2020) *Malware* [online] Available from: <https://us.norton.com/internetsecurity-malware-5-ways-you-didnt-know-you-could-get-a-virus-malware-or-your-social-account-hacked.html> [accessed 18 May 2020]

Spotting accounts/websites that have been compromised

Most website administrators will have some facility to monitor access to their site. For the RNA Community Site, I have an activity monitor where I can see attempts to log in to the website, this details the username, IP address, time and system used to get in. This is a handy tool as IP addresses can be 'banned' or locked out for certain periods of time (it may be a genuine user who has forgotten their password or mistyped it). A word of caution here though is hackers will hide behind false IP addresses so they will usually use another IP when banned.



The screenshot shows the 'Activity Monitor' interface for the RNA Community Site. The left sidebar contains navigation options: Dashboard, Home, Updates, Activity Monitor (selected), WP-UserOnline, Posts, Media, Link Library, Pages, FAQ, Historic Events, Comments, Everest Forms, Gallery, Lightbox, Appearance, and Plugins. The main content area is titled 'Overview' and includes a warning: 'This plugin is obsolete! If your webhost has PHP v5.4, use Plainview Activity Monitor instead.' Below this, there is a filter dropdown set to 'Nothing' and an 'Apply' button. The activity log table has two columns: 'Time' and 'Activity'. It lists several failed login attempts with red 'X' icons:

Time	Activity
3 days ago	bernie tried to log in to RNA Community Site IP 185.224.137.97 User agent Microsoft Office/16.0 (Windows NT 5.1; Microsoft Word 16.0.11001; Pro)
2020-05-14 03:58:03	KarlWebb tried to log in to RNA Community Site IP 185.224.137.225 User agent Microsoft Office/16.0 (Windows NT 6.2; Microsoft Word 16.0.11029; Pro)
2020-05-13 23:54:03	bob tried to log in to RNA Community Site IP 185.201.10.105 User agent Microsoft Office/16.0 (Windows NT 5.1; Microsoft Word 16.0.10827; Pro)
2020-05-13 20:40:35	geoff_a tried to log in to RNA Community Site IP 156.67.222.218 User agent Microsoft Office/16.0 (Windows NT 6.3; Microsoft Word 16.0.10730; Pro)
2020-05-13 18:57:34	grahamp tried to log in to RNA Community Site IP 92.249.45.41 User agent Microsoft Office/16.0 (Windows NT 10.0; Microsoft Word 16.0.9226; Pro)

Hacking attempts

The easiest way to spot websites and accounts that have been hacked tend to be the grammar and spelling, but this is not a rule of thumb as hackers are getting better at what they do.

How do I know if I have been hacked or have a computer virus?

Sometimes you will not notice a thing, but other people may (e.g. if they have received 'emails' from you sending them to unknown sites), but some common signs are³:

- You cannot log onto your computer, laptop, tablet, or smartphone, or on to your social media or online accounts.
- You see new icons or applications on your computer or mobile, or on the websites/accounts you use online.
- Files are missing, have been moved, or changed.
- You start seeing 'pop up' boxes on your screen; they may be offering help to fix your computer or may simply say 'close'.
- Money goes missing from your account(s).

³ Australian Competition and Computer Commission (2020) Scamwatch [online] Available from: <https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/hacking> [accessed 19 May 2020]

Preventing the Threat

There are so many warning signs that you may have been hacked, downloaded a virus, or are getting more and more spam through clicking website links. I have listed some of the basic things to look out for, but what do we do about preventing, or reducing the risks while online? Here are a few pointers:

- **Install Anti-Virus software** – there are so many paid and free Anti-virus software applications in use today. If possible, get a decent subscription as these will include regular updates of virus databases. The good applications will also include anti-malware, email scanning, password managers, Firewalls, etc. Most computers will come with pre-installed anti-virus software, but it is down to you to decide what suits you best. The free applications will give a basic level of protection, but this is better than not using anything at all. I have provided links to three main providers of paid software and one free application, but the choice is yours as to what you use.
- **Use your anti-virus software** – this may sound odd, but so many people will install anti-virus software but never run regular checks on your system. Use the software to scan for any virus that is already on your computer, after downloading a file that you then think may be suspicious, if your system slows down or shows odd behaviours. Your software can be programmed to run regular checks and should be monitoring your system all the time, but it always helps to scan regularly.
- **Keep your software and applications up to date** – When viruses and hacks are discovered with everyday software (e.g. Microsoft Office, Internet Browsers, etc.) the publishers will often ‘patch’ their software to counter the threat. You should ensure you update the software if prompted (from the provider, an email saying to update may be a scam).
- **Avoid using unknown networks (free wifi hotspots)** – a lot of places will offer free wifi access to the internet, these public hotspots can be used to access your system for personal information. If you are using a public network, you can hide your online activity by using a Virtual Private Network (VPN), further details on these can be found in the useful links section of this document.
- **Do not use easy to guess passwords on your accounts** – a lot of passwords are cracked through software or simply guessed. You should not use the same password for different accounts as if it is compromised, you could open all your accounts to the hacker. If you find passwords hard to remember, use a password manager, or use a combination of unrelated words, letters, and characters to form a password (e.g. Dog, Leander, Port could be written as **d0gLe@ndErpoRT** – note the use of capitals and lower case characters, and changing o to zero). Your anti-virus package may also offer a facility to generate random passwords for you. Do not write your passwords down and keep them with your device. If you must write a password down, keep it in a safe place away from any of your systems.
- **Manage your social media account settings** – it is a good idea to review your social media security settings (e.g. FaceBook settings that allow anyone to find you, switch this to Friends only). I would also switch off third party apps such as built-in games or advertising.
- **Always check the senders email address** – when you receive an email, check the email address belongs to the sender (e.g. you get regular emails from eBay: service@ebay.com a new email states your eBay account is locked, but the email address is accounts@ebayme.com is not from eBay – note ‘ebayme.com’).

- **Do not open unknown attachments, or click on unknown links in emails or websites** – If you have been sent an email, or social media message, with attachments or links from someone you do not know, do not click or open them, they may contain a virus or malicious code.
- **Report spam email** – most email providers have a spam filter, this will move emails with known keywords into a separate folder (note, check this folder regularly as you may find genuine emails may have been moved there). If an email looks like spam then it can be reported to the service provider, or to the National Cyber Security Sender (use the forward button and send the email to report@phishing.gov.uk).
- **Do not download ‘free’ software from unknown sources** – websites offering free software, music, movies, games etc, or free access to paid subscriptions, could potentially install software to your computer/device and access your personal data.
- **Lock your computer, laptop, netbook, smartphone** – if you use your device in public places, it is good practice to password protect your device, use a screen lock on your computer or device (if you leave your phone and it automatically locks after a set time, nobody can use it to view your personal data).
- **Back up your important data and files** – a good practice is to save a copy of any important documents, photographs, files onto a portable drive (USB drive, portable Hard drive etc.), or Cloud Storage (OneDrive, Google Drive etc). Keep this backup separate to your computer/device, it can be used to restore your data in the case of your system being compromised (even with a genuine hardware failure such as you dropping your computer, hard drive fails etc.)
- **Use Two-factor Authentication** – this is a little more advanced, but basically once you are identified as a known user in an account, you download an authenticator to you smartphone, when you log into a protected account (e.g. Facebook, Web hosting, etc.) you need to confirm a code shown on your phone. Anyone trying to hack your account would need your phone to authenticate themselves and be allowed access (see Useful links for a more detailed review of 2FA from the National Cyber and Security Centre).

If you have already been hacked, or have a virus on your system

How you respond to a cybercrime, infected or hacked system depends on what has happened. The National Cyber and Security Centre have several pages with further detailed information on what to do if you encounter a specific attack or problem (see useful links for Malware/Ransomware which takes you to the NCSC’s ‘actions to take’ on Malware/Ransomware).

The immediate action in these cases is to disconnect an infected computer/system from all network connections (wired, wireless or mobile phone based). You may want to switch off your wifi and disconnect other internet-connected devices in case they have been compromised.

Follow the guide as shown by the NCSC as there are many different courses of action to take depending on the situation.

As you can see, this is a massive subject to cover, I have given a detailed but basic guide, for further information please refer to the NCSC’s website (shown in useful links).

For awareness

Sadly, even before the current COVID-19 pandemic, other types of scams in operation are conducted over the telephone, by letter, or even on the doorstep.

- **Telephone Scams** – Cold callers are people or organisations that will ring known and/or random numbers in the hope of enticing you to part with personal information or money. They will often say they are police officers, network security officials, your bank, or other trusted companies. They may tell you details about yourself (such as your name and address) so you think they are legitimate, then they will ask for more details to ‘confirm your identity’ to pass on urgent information.
 - There are quite a lot of these scams and sadly, they are getting better at it all the time. The simple rule here is your bank, building society, internet provider etc, will not call you asking for details, if they are genuine then they will be happy for you to put the phone down and call a number known to you (e.g. the contact number on your credit card), preferably call the number using a different line (e.g. your mobile if they have called your house phone).
 - Never pass on any financial or personal details to anyone cold calling you.
 - Register with the Telephone Preference Service to limit companies cold calling you (sadly this will not stop illegal organisations contacting you).
- **Postal Scams** – Similar to the telephone scam, you may receive a ‘letter from HRMC’ or similar saying you have a refund due, or an outstanding debt. You will then be asked to log on to a website and confirm details, or send a cheque or BACS transfer of money to an account etc. Again, if genuine you can contact the service provider, HRMC etc, via a known number or address.
 - Register with the Mail Preference Service to limit junk mail (not addressed to an individual) and flyers.
- **Doorstep Scams** – The most brave scams tend to be people coming to your door offering services, or to let you know you have an issue with the roof/drive/garden and they can fix it for a fee. If there are more than one person, the worry here is they may be distraction burglars, one will keep you busy, the other will ask to go to the toilet or get a drink then look around for items to steal. Never let any cold callers into your property, ensure other doors are locked.

Golden rules

Regardless of the type of suspected scam, electronic, telephone, postal, or doorstep, always remember that anyone who is genuine will not mind you checking out that they are who they say they are.

Never give out any personal details such as passwords, pin numbers, account numbers, address, or date of birth. Always ask to see ID or confirm the identity of the caller from a known telephone number or email address.

Further information and useful links

National Cyber and Security Centre

This is the UK's authority on Cyber-crime. It has pages of useful guides on various aspects of cyber crime and how to secure your systems.

NCSC <https://www.ncsc.gov.uk/>

Anti-virus and security tools

Please note, this is not a recommendation of any product, I am just providing links to some of the popular software applications in current use.

Kaspersky <https://www.kaspersky.co.uk/>

Norton <https://uk.norton.com/>

McAfee <https://www.mcafee.com/en-gb/for-home.html>

Avast (Free) <https://www.avast.com/en-gb/free-antivirus-download>

Two-factor Authentication <https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa>

Virtual Private Networks <https://www.ncsc.gov.uk/blog-post/introducing-new-guidance-virtual-private-networks-vpns>

Malware/Ransomware <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

Telephone and Postal Preference Services (TPS and MPS)

TPS <https://www.tpsonline.org.uk/#>

MPS <https://www.mpsonline.org.uk/#>

Reporting Spam Email

Report spam email report@phishing.gov.uk

Webinar

The Fraud Advisory Panel and Charity Commission have an excellent webinar to help spot COVID-related fraud and provides practical advice and tips.

<https://gateway.on24.com/wcc/experience/elitebba/1917599/2071337/charity-fraud-awareness-hub>

Endnote

I hope you have found this document useful; the threat is changing all the time but hopefully by following some general rules you will be able to prevent some of the common attacks on your personal devices, data, or finances.

Yours Aye,

Karl

Karl Webb MA
Life Vice President
Huntingdon Branch
Royal Naval Association

MA Security & Intelligence Studies 2010

BUCSIS Research Fellow, University of Buckingham Centre for Security & Intelligence Studies (BUCSIS)

