A Silver Surfer's Guide to Staying Safe Online
The internet is a great way to stay in touch with friends and relatives, shop and pay bills online and do all sorts of research and planning such as booking holidays. However, with internet-related crime growing annually it’s important to be aware of the methods that hackers and fraudsters use to trick you into parting with information that they can then exploit.

This guide outlines the main threats, informing you about the things you need to be aware of. You’ll discover there is some cross over between the different threats, for instance, malware and fake website pages can be delivered by phishing emails. But once you familiarise yourself with the threats, you will be well placed to identify them.
Malware, or computer viruses as they are sometimes called, are rogue programs which can spread from one computer to another and steal personal information such as banking details and passwords. They are often delivered as an attachment via an email or a website link in an email. If you click on the link or open the attachment the malware downloads onto your device.

One of the most common and most dangerous types of malware is something called ransomware. This locks all the files on a computer, including photos and documents, and a payment is demanded to release the files. Other types of malware, such as spyware and key stroke loggers, record everything you do on a computer and sends it back to a server controlled by the hacker.
Phishing emails

Phishing emails are a huge problem. Millions are released each day globally and more often than not they hide different types of malware. They are designed to trick you into downloading an attachment or clicking on a link with some sort of urgent message.
For instance, around the holidays, you may receive an email saying you have a parcel waiting for you and you need to click the link to find out more. Another common phishing trick is an ‘invoice’ attached to the email. The message implies that you are due a payment, or even a tax rebate, but if you download the attachment, malware is released onto your computer.

Another common phishing trick is an email that purportedly offers health information, whether it’s about the seasonal flu, the latest virus going around, or advice on how to stay safe. Some will also offer to sell healthcare equipment at knockdown prices such as hand sanitizer.

Other tricks include phishing emails that claim you have won a lottery, cash prize, holiday getaway and so on. Phishing emails are also often themed to reflect calendar dates such as Easter, Christmas, and so on.

You can sometimes identify phishing emails because of poor grammar or spelling mistakes which suggest that the sender is not a native English speaker. However, that said, some phishing emails can be very professional and seem genuine.

The bottom line is that if you are not expecting an email and it comes as something of a surprise to you, treat it with caution. The general rule of thumb is that if it appears to be too good to be true, then it is probably fake. If you are uncertain, look for contact details and call the organisation by using the phone number found on their official website. Don’t use the contact details in the email as they are likely to be fake.
Phone scams

Another common scam is to receive a phone call from someone claiming to be from a well-known software company like Microsoft. They say there’s a problem with your computer and they need to get access to your computer to fix it.

This is a particularly nasty scam and there are established criminal gangs operating out of countries like India that run call centres dedicated to this type of fraud. First of all the fraudster will try and frighten you by saying you have a nasty virus on your computer or in some cases that you owe some money, to the tax office, for instance.

They will ask you to download some software that connects their computer to yours and you will see them moving the cursor about and opening and closing windows on your computer. They will then declare that they have found the virus and negate it and tell you to make some form of payment.

In the case of a request for money because of, for instance, purported non-payment of taxes, you will be asked to make a payment into an account.

Never let anyone download anything onto your computer. Keep in mind that not even Microsoft or any other company will know you have a virus on your computer or if there is some other problem.

And if someone tries to frighten you into making a payment you are not sure of, hang up the phone, and contact the organisation in question directly by getting the phone number from its website.
Video calls can be a lifeline for keeping in touch with friends and family, especially when someone is unable to leave home. There are a swathe of apps dedicated to video calls from Skype, WhatsApp, FaceTime, Zoom, Google Meet, and more.
They are safe to use but protective measures do need to be taken in order to keep safe. For instance, hackers may send phishing emails claiming to be from a video call app and ask you to click a link. The link takes you through to a page that appears to be from the app provider. However, it is a spoofed page, or fake page, created by the hacker to steal your ID credentials which will be used for criminal purposes at a later date.

To guard against this, remember that no company will ever ask a user to part with their password or ID details. These are private and belong to the individual. The company just supplies the app and never gathers your ID credentials.

Another important point is not to post video meeting details on social media. It might be tempting to do this, for instance, to family members and friends with meeting details so they can participate in a group call.

However, miscreants of various shades trawl social media for this information and will use it to interrupt meetings and cause trouble.

It’s also a good idea to use a VPN (virtual private network). This keeps your video connections and web browsing hidden from prying eyes ensuring you have private communications. It also keeps you safe from hackers by encrypting your data. Even if they were able to access your data they wouldn’t be able to make sense of it or break the encryption.
If something looks suspicious, such as offers that are too good to be true, or the grammar and spelling on the web page has mistakes, it’s best not to use the website. Always look for the padlock symbol in the browser bar which tells you that your data is encrypted and therefore safe from hackers. This method isn’t entirely fool proof but it’s generally a good safety indicator for e-commerce websites. The bottom line is always be cautious when entering your credit card details and personal information on a shopping website. Only do so if you are certain the website is genuine.

When it’s difficult to leave the house or you find yourself unable to get around much or your circumstances make it difficult to go to the shops, online shopping can be a good option. Online shopping for the most part is safe, however hackers do create fake websites that imitate a well-known shopping brand. This tends to happen during times of the year when there are big sales and more people are shopping online, such as Black Friday, Cyber Monday, at Christmas, or the New Year sales.

The golden rule is to use only shopping websites that you can trust and that you have successfully used in the past.
Fake websites and your banking information

Scammers also create fake websites that look official, requesting you to provide personal or financial information.

For example, a fake bank website may be set up asking you to update your account, password, or security information. Often they will look very similar to the real thing and only a few small details may be different.

Known as spoofs, the fake pages are typically delivered via email and you are requested to click on a link in the email. This will take you through to a web page that looks legitimate. In all likelihood you will be asked to enter your payment card details or bank account and sort code numbers and password.

Again, keep in mind that a bank, building society, an insurance company or some other financial services operator will never ask for your personal information such as a password or passcode. Have you ever spoken to your bank on the phone and been ready to divulge your password? The bank employee will always ask you to never tell them. It breaches security protocols and your password or passcode belongs to you alone. Certainly never enter it into a web page as this is what hackers are looking for and will try to get you to do.
Social networks are a good way to stay connected with friends and family especially during periods of isolation. To stay safe on these platforms don’t post personal information such as your physical address, when you’re not going to be at home, or other sensitive information.
Criminals and fraudsters do trawl these platforms looking for this sort of information, so to be on the safe side keep your posts general and if you do have private information to communicate use the private chat/message functions.

A further thing to be wary of is fraudulent adverts. These work in a similar fashion to phishing emails that try and lure you into clicking on them. If you do so, they typically take you through to a fake web page where they will try and get you to part with your personal information.

Use the privacy features on the website to choose who can see your profile and your posts. At the same time don’t publish personal identifying information such as your telephone number, address or date of birth. This type of information can be exploited by hackers.

In summary, on any social networking website, you must guard against people who want to steal your personal information, so never reveal personal information. Keep it general and keep it simple.
Keep your computer updated
Every computer has an operating system that controls the hardware and programs. Operating system manufacturers release updates when they discover security flaws. These updates are designed to protect the operating system and stop hackers from exploiting vulnerabilities. As such, it’s important to apply these updates as soon as you receive notification that they are available. Sometimes the updates are applied automatically and sometimes you need to apply them manually.

Privacy settings
On any social networking website, you must guard against people who want to steal your personal information. Use the privacy features on the website to choose who can see your profile and your posts. At the same time don’t publish personal identifying information such as your telephone number, address or date of birth. This type of information can be exploited by hackers.

Use security software
Good security software will look for and remove malware before it can infect your computer. It will also block unwanted adverts from popping up that can track your activities or scan your computer for personal information. It will also flag up phishing emails and warn you about websites that contain malware.
**Use strong passwords**

Many people use easy-to-guess passwords like ‘qwerty’ or ‘1234567’. This is dangerous because it provides easy access to the online services you use and makes it easy for fraudsters to pretend to be you.

Always use strong passwords that are hard to break. Ideally they should consist of at least 10 characters and be composed with a mixture of letters, numbers and symbols. Of course, this makes them hard to remember too but you can use a tool known as password manager that keeps them safe in a digital strong box. If you search online you will find plenty of options, including free password managers.

For extra security you can change your wireless router password. Wireless routers come with default passwords and it can be relatively easy for a determined hacker to crack these passwords. Your router should have come with instructions on how to change your password. If not, simply search online for the name of your router and the key phrase ‘how to change router password.’

Most online services also provide two factor authentication (2FA). 2FA provides an extra layer of security to your accounts to prevent someone from logging in, even if they have your password.

This extra security step requires you to verify your identity using a random code, for instance, delivered to your phone, each time you attempt to log into a service.

**Personal information**

There is a simple rule when it comes to protecting your sensitive data such as passwords, payment card details, bank account/sort code numbers and so on. Never reveal it to anyone online unless you are making payments on genuine websites.

This information is invaluable to cyber criminals and fraudsters and many of the online scams circulating today have the sole intention of getting this information somehow, whether it’s getting you to enter your personal information into a fake web page or planting malware on your computer.

By familiarising yourself with the tricks that hackers use, as outlined above, you will find it straightforward to protect yourself. But of course, you also need to be running basic cybersecurity such as antivirus software and a VPN because these are designed to keep you safe from the threats you can’t see.
Further information

Antivirus and identity protection

BullGuard provides easy-to-use award-winning products designed to protect you online and are simple to use. For example, BullGuard Internet Security and BullGuard Premium Protection both provide powerful protection against all forms of malware. They automatically detect, isolate, and block malware before it enters your computer. They also flag up unsafe websites that could be hiding malware and malware that is hiding in phishing emails.

BullGuard Premium Protection has the further benefit of providing identity protection. You simply provide the information you want to safeguard, such as passwords or payment card details, and it does the rest, scanning the internet 24/7 for your personal details. If your information appears anywhere online, it lets you know immediately so you can take appropriate steps.

Virtual private network

A VPN is an essential online tool to help you retain your privacy online and ensure your anonymity. BullGuard VPN creates a private tunnel between the computers you are using and the online services you access and also encrypts your data. It guarantees internet privacy and is particularly useful when using free public Wi-Fi hotspots, which are often not protected, and online services.

Action Fraud

Action Fraud is the UK's national fraud and cybercrime reporting centre. You can report all types of fraud whether it’s face-to-face interactions, over the telephone, or online. If you detect suspicious activity, it is better to report it as you may also help other people avoid becoming victims.

Age UK

Age UK provides further information about online fraud and an advice telephone line.