

BullGuard®



Silver Surfers' 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 people into parting with information that they can then exploit.

Malware

Malware, or computer viruses as they are sometimes called, are rogue programs which can spread from one computer to another or silently burrow into a computer 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.

One of the most common and most dangerous pieces 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.



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 need to get access to your computer to fix it.

They will ask for personal details. But even a big company like Microsoft isn't this omnipotent and it certainly wouldn't know if there is a problem with your computer. If you receive a call like this, hang up straight away.

A woman with short, curly grey hair is smiling and looking towards the camera. She is wearing a grey sweater and a necklace. She is holding a credit card in her right hand and has her left hand resting on her chin. In the background, there is a blurred view of a window with light coming through. A red banner is overlaid on the left side of the image, containing text about online shopping security.

Online shopping

Be cautious when entering your credit card details and personal information on a shopping website. Always look for the padlock symbol in the browser bar. This tells you if the website is secure.

Fake websites

Scammers also create fake websites which 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 or security information. Often they will look very similar, and only a few small details may be different.

Phishing mails

Fraudsters also send bogus phishing emails in the hope that people will enter their personal details. They may direct you to a fake website or trick you into thinking you've won a lottery or prize.

If you receive a suspicious email don't reply with your details or open any links or documents. Delete the email. If the email claims to be from an organisation, phone them directly using the phone number found on their official website and ask them.



Social networks

Fraudsters often use social networks such as Facebook to contact you and gain your trust. If something feels wrong, it probably is. These tricks can sometimes be hard to spot especially if things seem to be moving fast. Never send the person money or give them your account details.

How to protect yourself

1

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 mails and warn you about websites that contain malware.



2

Keep your computer updated

Every computer has an operating system that controls the hardware and programs. Operating system manufacturers release updates when they discover 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.

3

Use a strong password



If you have a wireless router, check that your wireless network is secure so that people living nearby can't access it. The best way to do this is change the 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.'

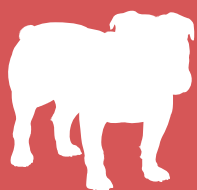


4

Social networks

On any social networking site, you must guard against people who want to steal your personal information. Use the privacy features on the site 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.



www.bullguard.com