




Tech Savvy Seniors

# Introduction to Cyber Safety







## How to stay safe online








Intermediate Guide



<b>TOPIC</b>	<b>INTRODUCTION TO CYBER SAFETY</b>	
<b>HOW TO STAY SAFE ONLINE</b>	The internet is just a part of life now, and there's so much you can do online. But should you trust the internet? The simple answer is yes. With the right tools and a few common sense precautions, you can protect yourself online. If you put security software on your computer and are careful about giving personal information to strangers, you should be just fine.	
<b>WHO IS THIS WORKSHOP FOR?</b>	You want to get onto the internet, but are worried that it's not safe. You want to understand and recognise the threats the internet might present, the measures you can take to avoid them, and the tools available to protect you and your computer.	
<b>WHAT YOU'LL NEED</b>	An internet-connected laptop or desktop computer; either your own or supplied by the workshop organisers. You may need to share a computer with others in the workshop.	
<b>WHAT YOU'LL LEARN</b>	This workshop covers the basics of internet security: the things that can potentially go wrong and the simple steps you can take to help avoid them.	
<b>TIMETABLE</b> The workshop will be broken into five topics, with a break in the middle. Feel free to ask questions at any time. 	<b>SUBJECT</b>	<b>DURATION</b>
	Do I need to protect myself on the internet?	10 minutes
	The threats you might face	30 minutes
	What does security software do?	20 minutes
	Choosing security software	15 minutes
	<b>Break</b>	<b>15 minutes</b>
	Keeping yourself safe (security software is not enough)	40 minutes
	<b>Summary</b>	<b>10 minutes</b>
	<b>TOTAL</b>	<b>140 minutes</b>

©2022 edition

SUBJECT	DO I NEED TO PROTECT MYSELF ON THE INTERNET?
TIME 	10 minutes
OVERVIEW 	<ul style="list-style-type: none"><li> Has something bad happened to you or someone you know online?</li><li> Are your computers and your wireless networks password-protected?</li><li> Have you given private, compromising details to strangers online?</li><li> Do you have security software installed?</li></ul> <p>This workshop is about making you aware of some of the risks that exist on the internet, and the precautions you can take to help defend yourself against them. It's not really that hard to keep yourself safe, you just need to follow some simple rules.</p> <p>The first part of the workshop explains some of the dangers you may encounter online. There are really just a handful of key threats, and knowing what they are can help you to understand safe and unsafe actions when you're accessing the internet.</p> <p>A key element of keeping yourself safe online is the idea of trust, and we'll look at this quite a bit more as the workshop continues. On the internet, anybody can falsify their identity, so you need to know who you should accept emails from, where it's safe to shop, and to whom you should give your details. A few commonsense steps will make you difficult to scam.</p> <p>Just as important as your online behaviour are the tools that help protect your computer and personal information. The second part of the workshop covers the role that internet security software plays in keeping you safe from cybercrime.</p>

SUBJECT	THE THREATS YOU MIGHT FACE
TIME 	30 minutes
<b>MALWARE</b> 	<p>Let's look first at some of the bad things that can happen. For most people, there are three key dangers to be aware of: malware, hackers and identity theft.</p> <p><b>Malware</b> (malicious software) is created with the intention of accessing your computer and gathering information, usually for the purpose of selling to other interested parties. The most commonly known type of malware is a <b>virus</b> (and the two terms are often used interchangeably) but others include <b>spyware</b>, <b>adware</b>, <b>worms</b> and <b>Trojan horses</b>. Malware can do a variety of things, including:</p> <ul style="list-style-type: none"> <li> Spying on your activity (spyware)</li> <li> Letting someone remotely control your computer</li> <li> Actively damage your files and computer</li> <li> Spread infection to other files and computers (virus, worm)</li> <li> Force you to watch ads (adware).</li> </ul> <div data-bbox="443 1037 1165 1303" data-label="Image"> <p>The screenshot shows the Windows Defender interface. On the left, it says 'Viruses detected (5)' and 'Your computer is infected with dangerous viruses'. Below that, it says 'Click "remove viruses" and remove all viruses remove viruses'. On the right, it says 'Virus &amp; threat protection' and 'Actions needed in Windows Defender'. Below that, it says 'Windows Defender Antivirus found Trojan:Script/Cloxxer.A!cl in PowerShell_C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe_10.0.16299.15000000'. At the bottom, there are 'Read more' and 'Restart' buttons.</p> </div> <p>You'll nearly always get malware by running an infected application. The app itself will probably work exactly as normal; it just secretly installs a virus, spyware or adware onto your computer when it's run.</p> <p>That's how the malware writers grab you: they take an app that's appealing to you and slip a virus, spyware or adware into it. That's why they are often called Trojan horses.</p> <p>This is why you need to be careful about which apps you download and run on your computer. If you download an app from a disreputable source, it may be infected.</p>

Malware can introduce a virus to your computer.

## HACKERS



The term **hacker** is really something of a misnomer, since there will almost never be a person trying break into your computer system. But there are automated programs called **bots** that might try and test your computer's defences.

Even these are vanishingly rare now, since most computers have excellent defences against virtual intruders. It's highly unlikely that your computer is vulnerable out of the box unless it is very, very old.

What a hacker (or bot) does is try to exploit a vulnerability in your computer's security.

As an example, do you know about Windows file sharing? This allows one computer to send documents to another computer over a network. But if it's not password protected, a hacker might detect that and use it to access your files or implant a virus or other type of malware on your computer.

## IDENTITY THEFT, PHISHING AND SCAMMERS



There are no rules about who you can say you are on the internet, so people can try to pretend they're something or someone they're not in order to get you to give them money or reveal personal information like credit card numbers and online banking logins.

Essentially, con artists have taken their business online, and they're trying to take advantage of you.

A common scam is the **phishing** attempt, where the scammer pretends to be a person or organisation that you have a relationship with, and gets you to give up private information, like your bank account details. The next pages show examples of phishing emails.

### Phishing, a classic example

An example of **phishing** is the online banking scam. In this case, the victim receives an email that looks like and purports to be from their bank. It often has some dire warning about their finances, and says they need to log on to their online banking service in order to fix it. A web link is embedded in the email.

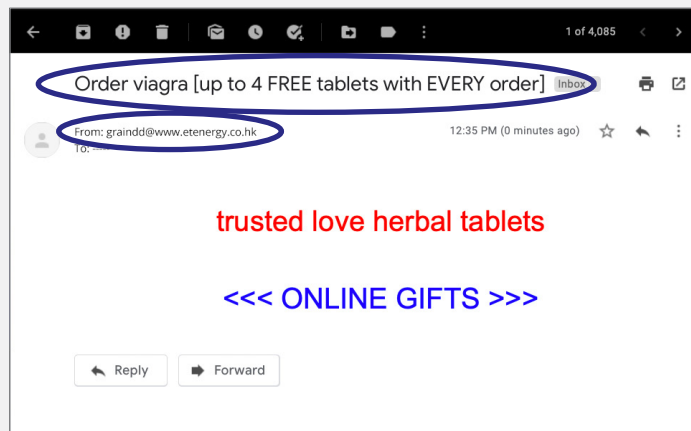
The link does not lead to the real bank's site, however, but to another site that's made to look exactly like that of the real bank. The person would only know if they looked at the web address in the browser address bar. Then, when the victim logs in, their internet banking password is taken by the scammer. Sometimes bogus emails can appear to come from the tax office, a courier service or a utility provider.

## HOW TO SPOT PHISHING EMAILS

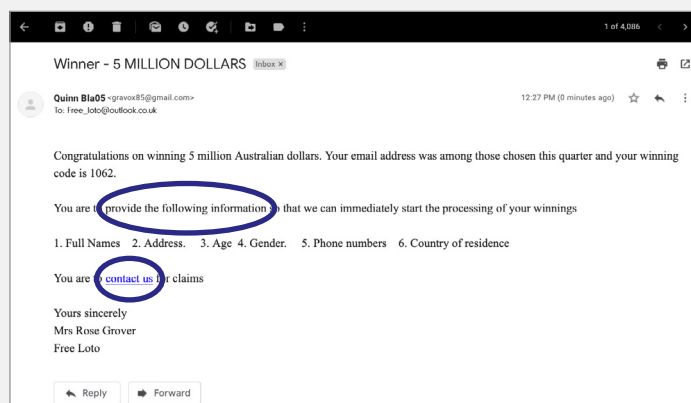
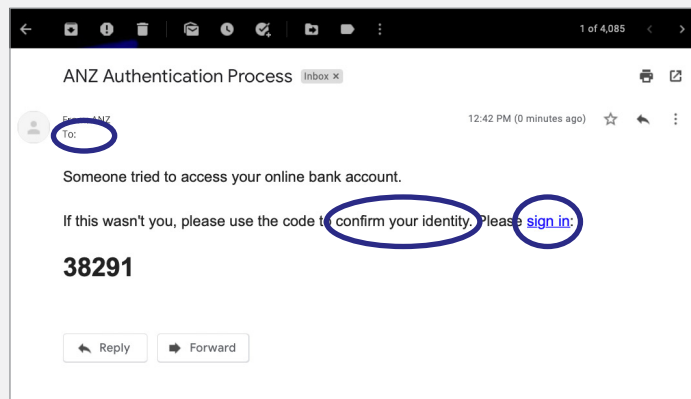


There are some simple ways to help identify spam and phishing scams, and avoid getting into trouble on the internet. Here are a few things to look out for.

Check the email's subject and sender. Is it from someone you know, and does it describe something you remember signing up for? If not, it's probably spam.



Is there an offer of free money in exchange for your personal information? Does it sound too good to be true, or threaten consequences if you don't respond with personal information, or by clicking or link? Does it not have your name in the **To** field? These are all signs of a phishing scam.

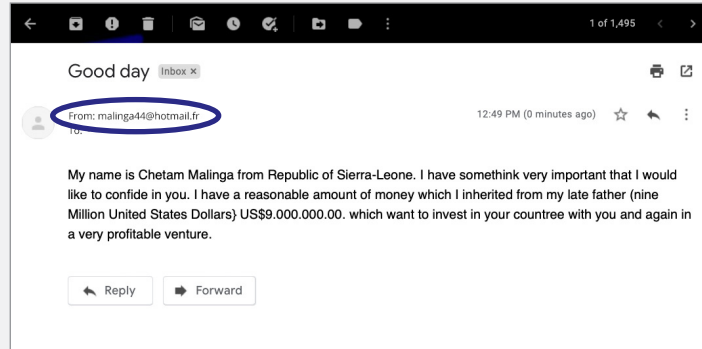


## HOW TO SPOT PHISHING EMAILS



Does the email contain spelling and grammatical errors, and is it poorly presented? Is it from a 'free' email account (outlook.com, yahoo.com, gmail.com)? If it is, and you don't know the sender, treat it with suspicion.

**Vanity scam** emails like the one below can be very appealing, and many look authentic. Be sure to question why you'd be receiving such an email, such as names, addresses and websites. Security software can't always protect you if the goal is to trick you rather than infect your computer.




SUBJECT

WHAT DOES SECURITY SOFTWARE DO?

TIME 

20 minutes

TYPES OF SECURITY SOFTWARE 

The good news is that you can protect yourself from most attacks using security software. Your computer comes with some security software built-in, but you should add additional software on top of that. There are different types of security software you can get:

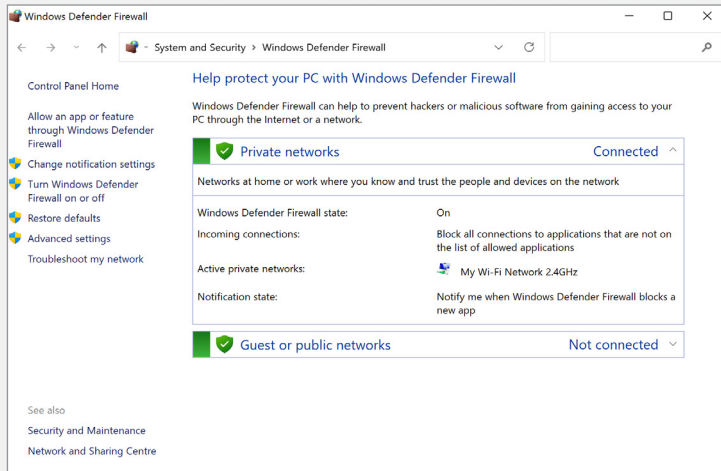
- ▶ **Antivirus:** Software that protects your computer from most types of malware (and relies on your computer’s built-in defences for the rest). You can get antivirus software for free or a small charge.
- ▶ **Internet security suites:** A package of software that protects your computer from a whole range of threats, including malware, scammers, junk email, trick websites, hackers, and much more. Internet security suites have an annual fee (usually between \$60 and \$130).

PROTECTING YOUR COMPUTER 

To break it down a little more, defending your computer from internet threats involves a number of elements:

- ▶ **A firewall** acts like a security checkpoint for internet traffic – it only allows authorised traffic through. If somebody outside tries to talk to your computer without authorisation, they can’t. If an app on your computer tries to talk to the internet, it will either be stopped, allowed, or a pop-up will appear asking you if you’d like to let the program communicate with the internet. On a Windows PC, the pop-up will look like the image below.

Your computer comes with a firewall built in.



← A firewall blocks access to your computer.



## PROTECTING YOUR COMPUTER



- ▶ **Antivirus** software tracks down and removes any malware – including viruses, spyware, and adware – that comes onto your computer. Your computer likely does not come with antivirus software, and you should install it.

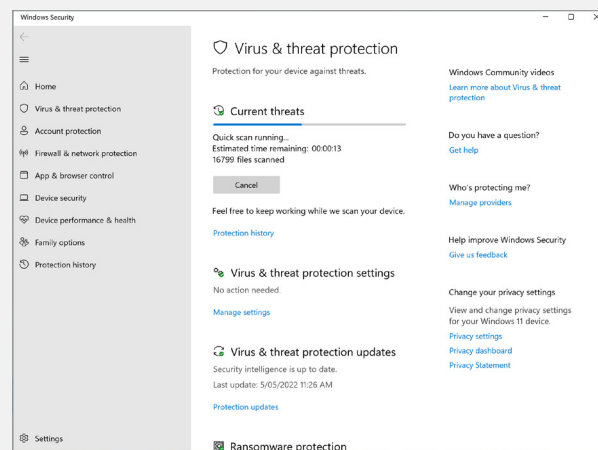
Those are the key elements of security, but an internet security suite can offer an even broader range of protections, including:

- ▶ **Parental controls**, which prevent websites with objectionable content (like offensive language and pornography) from loading on your computer
- ▶ **Backup**, which automates the backup of your important data to external storage devices
- ▶ **Spam filters**, which prevent scam and junk email from reaching your inbox
- ▶ **Web filters**, which prevent you from visiting the websites of known scammers
- ▶ **Identity theft protection**, which prevents personal data from being sent over the internet.

## HOW TO USE PROTECTION



Mostly you don't have to do much to use either internet security suites or standalone anti-virus software. They usually run in the background of your computer, and the only reason you'll know they're running at all is that there will be a small icon at the bottom of your screen. If you double-click on that icon, you can see the full





← Home screen of a security software program.

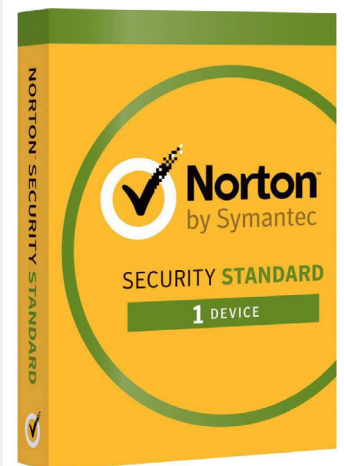
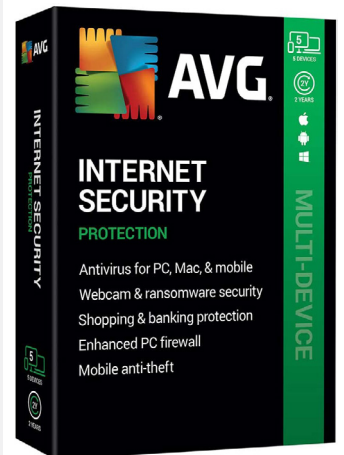
interface for the security software.

You probably won't have to do that very often (if ever) – security software is mostly automatic.



It's likely you'll only know that security software is running when something bad happens (for example, when it detects a virus), and a pop-up will appear asking you what you'd like to do about it.

If you have time, your presenter can show you a simple antivirus application (such as Microsoft Security Essentials) being installed.

SUBJECT	CHOOSING SECURITY SOFTWARE
TIME 	15 minutes
OVERVIEW 	<p>It's recommended that any device you connect to the internet – your PC, tablet or smartphone – be protected with antivirus software or, ideally, an internet security suite.</p> <p>If you are unable to afford the annual charge, you can get a free antivirus application instead. It won't protect your system as well as a security suite, but it will offer you a baseline of protection.</p> <p>Some makers of internet security suites include:</p> <ul style="list-style-type: none"> <li>▶ Norton by Symantec: <a href="http://au.norton.com">au.norton.com</a></li> <li>▶ McAfee: <a href="http://www.mcafee.com.au">www.mcafee.com.au</a></li> <li>▶ BitDefender: <a href="http://www.bitdefender.com.au">www.bitdefender.com.au</a></li> <li>▶ Trend Micro: <a href="http://www.trendmicro.com.au">www.trendmicro.com.au</a></li> <li>▶ AVG: <a href="http://www.avg.com.au">www.avg.com.au</a></li> <li>▶ Telstra Broadband Protect: <a href="http://www.telstra.com.au/broadband/extras/broadbandprotect">www.telstra.com.au/broadband/extras/broadbandprotect</a></li> </ul> <p>Most of the above software companies also sell cheaper, standalone antivirus solutions.</p> <p>If you can't afford a security suite, Windows Security is built in to Windows 11 and Windows 10. Alternatively you can get a free antivirus app from:</p> <ul style="list-style-type: none"> <li>▶ AVG: <a href="http://www.avgfree.com.au">www.avgfree.com.au</a></li> <li>▶ Avast!: <a href="http://www.avast.com">www.avast.com</a></li> <li>▶ Comodo: <a href="http://antivirus.comodo.com">antivirus.comodo.com</a></li> </ul> <p>When comparing security suites and free antivirus tools, check how much each costs and if they have the features you need:</p> <ul style="list-style-type: none"> <li>▶ Does it have automated backup?</li> <li>▶ Does it have online backup? (Which is storing your files on an online server)</li> <li>▶ Does it have parental controls?</li> <li>▶ Does it have a spam filter?</li> <li>▶ Does it have a firewall?</li> <li>▶ Does it tune up your computer and test for vulnerabilities?</li> </ul>



A security suite helps protect you and your devices from threats on the internet.

SUBJECT	KEEPING YOURSELF SAFE
TIME 	40 minutes
SECURITY SOFTWARE IS NOT ENOUGH 	<p>Installing security software on your computer is a big and important step in protecting yourself online. But that's not the whole solution: security software can't protect you from con artists and cyber criminals.</p> <p>Many things we do online involve information that's important, personal or private. Your personal information is information that identifies you. In order to protect your personal information, you should be careful about what you share publicly online. Common sense and a healthy dose of suspicion will make you very difficult to scam!</p> <p>There are some simple things you can do to keep yourself safe:</p> <ol style="list-style-type: none"><li><b>1. Use a strong and unique password/passphrase, and change it regularly</b> Creating a strong, unique password for every online account is key to improving your online safety. A strong password is long (more than 12 characters) and contains a random mixture of letters, numbers, symbols and capitals. Your password should be different for every site. Typing out three or four words – what's known as a passphrase – can often feel more natural than a complex combination of letters, numbers and symbols. Add a few capitals and punctuation and you have a strong and easy-to-remember passphrase. Use it where a site permits a longer number of characters.</li><li><b>2. Use more than one kind of security for your devices</b> To keep your devices as secure as possible, use as many security features as you can. Depending on your brand of device, this might include a passcode, a PIN, and biometric security such as your fingerprint or face. To use payment features and access banking and other financial services, you might be required to set up biometric security. Using multiple security features will protect your device and personal information.</li><li><b>3. Set up two factor authentication (2FA), if available</b> Many accounts and services now give you the option to protect your password with an extra step. When you enter your password, a code will be sent to your nominated mobile device or email address. You'll need to enter this code to continue. When 2FA is set up, even if someone finds out your password, they still won't be able to access your personal data.</li></ol>



#### 4. Use a password manager

A password manager is a special account that remembers and secures all your passwords. It is secured by a master password, and means you don't need to remember lots of passwords or risk accidentally using the same password for multiple accounts. Your web browser includes a basic password manager, which is free. You can also purchase a standalone password manager that can sync passwords between different browsers and devices, as well as alert you when a password might have been compromised.

#### 5. Keep your device up to date

System updates for your computer and mobile devices are provided by the manufacturer of your device. You'll see an alert on your computer or mobile device whenever an update is available, and you should always install it as soon as possible. Updates improve the security of your device, and may bring performance improvements too. Your device also has an app or setting where you can check for any updates you might have missed. If your device is very old – usually 10 years – you might get an alert from the manufacturer that updates will no longer be provided. Your device will still work, but you should take this as a signal: It's time to upgrade!

#### 6. Don't post personal information on public sites

Lots of sites would like you to give them your personal information: name, date of birth, address, email address and so on. In some cases, such as shopping sites, it's necessary and legitimate. On others, like Facebook, you don't need to (and should not) provide private information, so restrict who can access your posts in the privacy settings.

#### 7. Don't open email attachments unless you're really sure

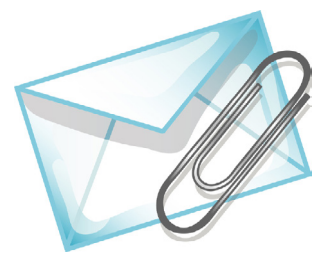
One of the most common sources of malware infections is email attachments. Email attachments are files that come with emails on your computer.

If you remember what we said earlier about you needing to run a program to get infected with malware, this is how you often get trapped: an email will come in with a program attached and some kind of exhortation to run it, like **Run this program, it's awesome!** Instead of opening an attachment, the email might ask you to click on a link which takes you to a website that will try to infect your computer.

These can even come from people you know and trust. They might send you the malware not knowing it's adware or spyware. There is also a type of virus malware which can actually hijack the email of infected computers and send out copies of themselves to everybody in the infected person's address book.



Don't publish private information to social media sites.



Be careful about opening email attachments



The short of it is, if you're not sure, don't open the attachment.

That's not to say don't use email attachments. If you receive a specific document or picture that you're expecting, it's fine to open it.

**8. Be careful about what emails you respond to**

Emails can be made to appear as if they come from anybody, kind of like letters with a fake sender address.

If an email asks you to give up information, follow a web link to an external website or anything that seems shady, don't respond to it. Don't engage at all; delete it and move on.

If you're really worried – for example, if you get an email from your bank – you can always call them or manually go to their website (don't follow the link from the email).

**9. Be careful who you give credit card details to**

One of the great things about the internet is that it's the world's largest shopping mall. Hundreds of thousands of stores around the world are a click away. But not all of them can be trusted.

If you're not sure about a given store, it's a good idea to do a Google search on the name of that store, which can give you background information on it. If it has a bad reputation, a Google search will likely reveal it.

Services like PayPal allow you to buy things without giving up credit card details to a store. We cover that more in our **Online Shopping and Banking** workshops.

**10. Don't install apps from untrustworthy sources**

Malware generally comes attached to other (legitimate-looking) apps.

When you download an app from a shady source, you run the risk of downloading malware.



Do not click on links in suspect emails – delete the email.



Use services that don't involve sharing credit card details.



Research suspect programs or sites

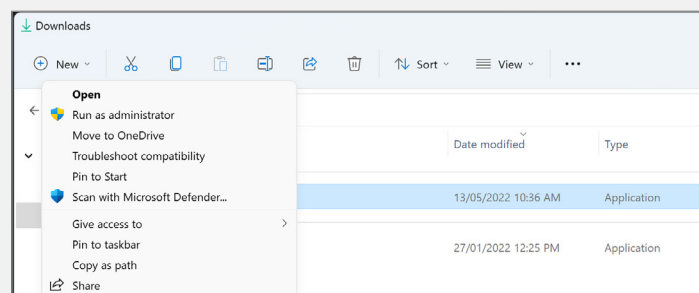
## SECURITY SOFTWARE IS NOT ENOUGH



How do you know if a site or app is shady? One good way to find out is to run a Google search on the site name or file name to see if anybody else has had problems.

If the site has user comments, you can also check those. If the app is infected, somebody might have noted it.

- ▶ After downloading an app, you can run a virus scan on it immediately. Malware is not active until you actually run an app. If you use a Windows computer, go to the folder that you downloaded the app to. Right-click on it, and select **Scan with... [name of antivirus app]** from the drop-down list. To see the list you might need to click **Show more options** first

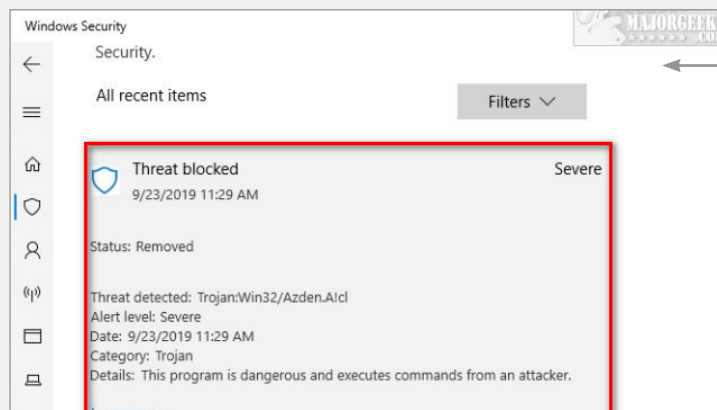


Run a virus scan when you download an app.

## WHAT HAPPENS IF I GET INFECTED?



If your security software does find malware, it will likely ask you what to do with it. A pop-up will appear on your computer looking something like this:



Security software can delete or isolate potential threats.

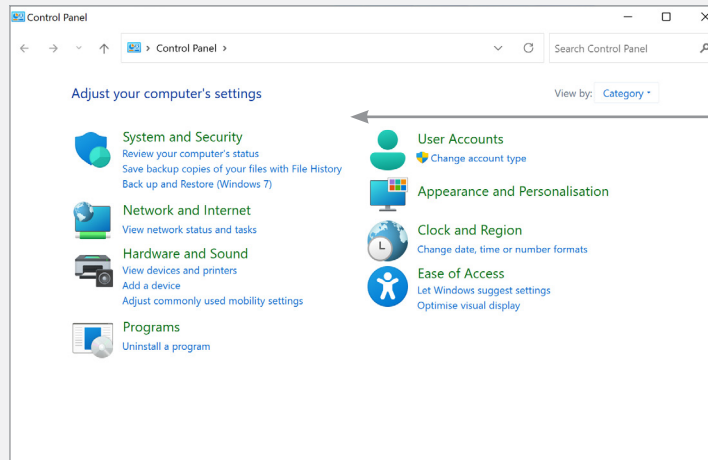
Don't panic – this is the security software working. Generally you want to remove or quarantine the malware. Choose the option to do so. That should remove the virus and the threat. Problem solved.

Even so, it's always a good idea to make copies (backups) of the files and photos you think are important! If you have a flash drive or an external hard drive, you can make a copy onto that, or you can backup to the cloud if you have cloud storage. If you bought an internet security suite, it might have a backup tool built-in.

## WHAT HAPPENS IF I GET INFECTED?



Alternatively, you can use your computer's built-in backup system. If you have a Windows computer, click on the **Start** button (or Windows icon) on the bottom left, then on **Control Panel**. Then select **Back up your Computer**. Windows will walk you through the backup process.



Many computers have built-in backup features.

## Why annual fees?

Internet security suites nearly always charge an annual fee, rather than a straight-up, buy-once price. That's because the software has to be continuously updated to protect your computer from new threats. You can think of it like a flu shot: just as we should be vaccinated each year against new strains of a virus that can make us sick, so should our computers.

## SUMMARY

This was a tough workshop, and if you have any questions, feel free to ask!  
Here's a summary of what you've learned in today's session:

### TIME

10 minutes

### RECAP



- ▶ What malware is
- ▶ What a hacker does
- ▶ What a phishing scam is
- ▶ What security software does
- ▶ The different elements of a security software suite
- ▶ Commonsense things you should do to protect yourself online.

### USEFUL WEBSITES



If you want more information on staying safe online, be sure to check out:

ID Support: [www.nsw.gov.au/id-support-nsw](http://www.nsw.gov.au/id-support-nsw)

Free call 1800 001 040 Monday to Friday from 9am to 5pm for advice and guidance on how to deal with compromised documents, how to keep your information safe, and how to access additional support such as counselling.

Telstra's Cyber Safety site: [telstra.com/cybersafety](http://telstra.com/cybersafety)  
Information and top tips for securing devices and helping protect personal information.

Australian Cyber Security Centre: [www.cyber.gov.au](http://www.cyber.gov.au)  
The Australian Government's online safety and security website.

Telstra Broadband Protect: [www.telstra.com.au/broadband/extras/broadbandprotect](http://www.telstra.com.au/broadband/extras/broadbandprotect)

Helps protect you and your family on devices connected to your Telstra home broadband service, without needing to install any software.

Google Safety Centre: [www.google.com.au/intl/en/safetycenter](http://www.google.com.au/intl/en/safetycenter)

Simple and easy-to-understand information on staying safe and secure online.

Scamwatch: [www.scamwatch.gov.au](http://www.scamwatch.gov.au)

Information about how to recognise, avoid and report scams, plus updates on the latest scams.

If you or someone you know has been scammed and are experiencing personal distress, contact:

Lifeline: [lifeline.org.au](http://lifeline.org.au)

Beyond Blue: [beyondblue.org.au](http://beyondblue.org.au)



## GLOSSARY



TERM	EXPLANATION
ADWARE	A particular type of viral infection that forces you to watch ads.
ANTIVIRUS	A program that hunts down and removes viruses from your computer.
BACK-UP	Making a copy of important files, in case the originals are lost.
BACKUP PROGRAM	A program that automates backup, performing a backup at fixed intervals.
BOT	An automated program. Most 'hackers' are actually bots – programs that automatically test internet-connected computers for vulnerabilities.
CLOUD	A remote server that stores your data. Keeping data in 'the cloud' instead of on a computer allows you to access it from any internet-connected device.
EMAIL ATTACHMENT	An image, program, document or file that's embedded in an email message.
FIREWALL	A defensive program that blocks unauthorised internet traffic.
HACKER (OR CRACKER)	A person who tries to break into computer systems.
IDENTITY THEFT	Pretending to be someone else online in order to access personal details and financial services.
MALWARE	A catch-all term for malicious programs that harm your computer. Often used interchangeably with virus.
PARENTAL CONTROLS	Filters that prevent users of a computer from accessing objectionable content.

## GLOSSARY



TERM	EXPLANATION
PHISHING	A particular type of scam, where an email or web message is used to try and trick people into revealing their passwords, personal or financial information.
POP-UP	A small notification box that appears onscreen. Security software uses pop-ups to let you know something has happened and ask what you'd like to do about it.
SECURITY SUITE	A comprehensive set of tools for protecting you online. They include antivirus, malware, firewall, spam filters and more.
SPAM	Unwanted email.
SPAM FILTER	A program that stops spam from reaching your email inbox.
SPOOF	Pretending to be someone else or a different site. For example, an email spoof pretends to be from someone you know, but is really from a stranger.
SPYWARE	A type of malware that monitors your activity on your computer. It can be used to find out what your passwords are, for example.
VIRUS	A program that takes control of your computer without you knowing about it.