

Video transcript - Episode 1: Online security

WARREN PERUMAL

EXECUTIVE MANAGER – ONLINE BANKING SECURITY

It's incredible to think the Internet, as we know it, is less than 30 years old. For most of us, imagining life without the Internet is almost like imagining life without electricity.

The Internet has brought us email, access to the world's information at our fingertips and the ability to keep in constant connection with our family and friends around the world. And it's changing the way we do everyday things like reading the news, booking flights and, of course, doing our banking.

But, just as with electricity, along with the great benefits of the Internet, there are some basic precautions you need to take to stay safe.

There are two main things you need to do to help keep your online experience safe.

Protect your computer from viruses, and avoid giving out your personal details and passwords.

There are many different types of computer virus with a range of names like trojans or worms. They all operate in different ways but essentially they are computer programs that use the Internet to get into your computer.

Once in your computer they can do pretty much anything the virus creator programmed them to do – like wipe the contents of your hard-drive, make your computer run slow, email spam, including sending the virus to everyone in your address book.

Some viruses can track the information entered into your computer, such as passwords, login IDs and credit card details - and send the information back to online criminals. Even if you are very careful about how you use the Internet, it is still possible to get a virus without realising it.

The best way to protect against getting a computer virus – or to remove an existing virus is to install a current antivirus program. Antivirus programs are easy to install and can be purchased online and downloaded straight to your computer – or disks can be purchased in stores selling computer software. Once installed, you should ensure you have the automatic updates feature turned on to keep your computer protected against new viruses.

Just make sure you purchase your antivirus software from one of the well-known brands, because one tricky way of getting viruses on computers is to disguise the virus as antivirus software. Links to reliable antivirus software brands are available on the commonwealth bank website.

If you don't feel comfortable installing antivirus software yourself, companies like McAfee provide a service where they access your computer, remove existing viruses and install antivirus software for you.

Along with installing antivirus software, you should make sure your computer operating software is up to date by always installing the free updates, such as those from Microsoft or Apple when they are released. As well as providing regular security fixes, these updates often include software improvements, bug-fixes and new features that will make your computer run better overall.

The other part of good online security is to be aware of the information you share online. Do the billboard test. Would you be comfortable if all your Facebook information was on a billboard on the street for anyone to see?

Information like your birthday, place of birth, mother's maiden name and other standard identification questions shouldn't be shared. Make your profile private and only add friends you actually know.

Only ever enter your ID and passwords into websites you have navigated to, and never from a link in an email. Links in emails may look familiar but could actually take you to a fake version of the website you wanted. The fake website could be designed to capture your ID and password – or to download a virus to your computer.

The Commonwealth Bank will never ask for your online banking log in details or any of your personal information in an email. If you receive an email from the bank asking for this information, it's a fake – no matter how convincing it looks.

Look for the https prefix instead of the regular http. The extra "s" indicates a secure connection where your password and other details will be encrypted and more secure when being entered over the web. You should also look for the https in the address bar of any website you enter your credit card details into.

In general scam artists and cybercriminals can only affect you if they have your personal details. And despite the high-tech world we live in, by far the most common method they use to get your details is basic deception; tricks to get you to unwittingly hand over the information yourself. Knowing this helps you to think more carefully before responding to online requests.

The old adage that if it seems too good to be true then it probably is, certainly applies to online and email offers. So treat them all with great caution. When in doubt about any online request, even those that appear to come from trusted organisations or friends don't respond unless you can verify that the request is genuine.

It's not hard to protect yourself online. It's a matter of taking simple steps like installing virus protection software and applying the same caution and common sense with revealing personal information online as you would in the real world.

You can find out more information about online security on the Commonwealth Bank site by clicking on the security link. Also take a look at the next video in this series where I talk specifically about how safe it is to bank online with NetBank.

(LOGO: Commonwealth Bank)

(SUPER: DETERMINED TO BE DIFFERENT)

(SUPER : To find out more, visit
commbank.com.au/security)