**CYBER SECURITY FOR SENIOR CITIZENS**

**What is a Squeeze Page?**A type of social engineering in which a person is informed they have won a prize or can gain some useful information which triggers greed or curiosity in the person. They are instructed to click a link to receive the prize or access the information at which point a form loads requiring them to provide personal information before they can receive it. The gift cannot be accessed or downloaded until the information has been supplied. This process also allows identity thieves to covertly place a key logger on the person’s computer during the download of the free gift.

**If we click on links in emails from unknown origins what are the potential risks?**Cyber criminals rely on peoples’ lack of awareness and trusting nature to commit cyber-crime. Clicking on suspect links allows the criminally inclined to covertly place a key logger or virus on the person’s computer during the download.

**Why is it good practice to check your bank statements regularly?**
Cyber criminals steal account information and use a victim’s own financial resources to purchase goods online and or to pay for services without the victim’s permission or knowledge. By checking your statements regularly, you will be able to spot unsuspected or suspicious charges you did not make. If you see anything suspicious on your bank statements, contact your bank immediately.

 **What is a Key Logger?**
Keystroke logging is a criminal covert action designed to steal passwords and other personal data unique to an individual or groups of individuals, such as a family. The keystroke logger is a small software application that is covertly located onto a person’s computer. From that point on every key stroke generated by the person using the computer is recorded and sent to the criminal or criminals seeking the data collected by the key logger.

**What should we do if we receive a cold calling phone call?**
Usually a criminal contacts the intended victim by phone and informs them that their computer is infected with a virus, or that they can check or service their computer. The victim is instructed to give the criminal remote access to their computer so that they can fix it. Once they gain access personal data is stolen which allows them to commit a criminal act against the victim. Cold callers may even try to get you to give up identity information about yourself by answering questions they claim are for a survey they are doing.

Don’t speak, just hang up and then tell a friend or family member about it. If it keeps happening record the date and time and contact your service provider. Never follow instructions to open up your computer if the caller informs you that they can tell that you have a computer related issue.

**Why do criminals like the Internet?**Because it is a target rich, offender-friendly environment.

[**www.cert.govt.nz**](http://www.cert.govt.nz)

CERT NZ is your first port of call when you need to report a cyber security problem. They support businesses, organisations and individuals affected by cyber security incidents, and provide trusted and authoritative information and advice.

**“Remember if we stay in our bubbles, we will have less troubles”** John Parsons C21