IDENTITY THEFT

Identity theft is when a cybercriminal gains access to your personal information to steal money or gain other benefits. They can create fake identity documents in your name, get loans and benefits or apply for real identity documents in your name, but with another person's photograph.
The financial and emotional consequences can be devastating for victims. Once your identity has been stolen it can be difficult to recover and you may have problems for years to come.

What type of information do cybercriminals steal?
A cybercriminal may look to steal a range of personal information including:

- Name.
- Date of birth.
- Driver's licence number.
- Address.
- Mother's maiden name.
- Place of birth.
- Credit card details.
- Tax file number.
- Medicare card details.
- Passport information.
- Personal Identification Number (PIN).
- Online account username and login details.

How do you know if your identity has been stolen?
Look out for these common warning signs:

- Your bank statements show purchases or withdrawals you have not made.
- You stop receiving mail you may be expecting (e.g. electricity bills) or receive no mail.
- You receive bills or receipts for things you haven't purchased or statements for loans or credit cards you haven't applied for.
- A government agency may inform you that you are receiving a government benefit that you never applied for.
- You have been refused credit because of a poor credit history due to debts you have not incurred.
- You may be contacted by debt collectors.

What to do if you think your identity has been stolen
If you suspect any fraudulent use of your identity, there are some steps you should take:

- Immediately report it to your bank, local police, social media account's website or other online account that you may be concerned has been hacked into (these sites usually have a 'Help' section where you can report fraudulent activity to and seek help).
- Change the passwords on your accounts and close any unauthorised accounts.

HACKING

Hacking refers to unauthorised access of a system or network, often to exploit a system's data or manipulate its normal behaviour.
Now a common part of our vocabulary, we read about hacking daily as data spills and breaches make headlines, and major organisations warn their customers to check their bank statements carefully.
While it's often a catch-all term applied to anything that compromises or negatively affects our computers, 'hacking' represents a particular kind of threat to your network and accounts.

How it works
Like breaking into someone's home, thieves have to look for a way in. Using software code, either developed themselves or available in a ready-to-use kit online, hackers look at ways to gain access to a network. Often finding out a password is the first step in cracking a network's security. Once in, a hacker can modify how a network works, steal data, obtain passwords, get credit card information, watch what you are doing or install malicious software (malware) to further the attack.
While hacking is often highly targeted, some hacking tools such as ransomware or phishing malware can spread on their own via links and attachments. Malware can compromise your system or accounts without someone specifically targeting you.

How to protect yourself from hacking

- Install anti-virus software on all devices and set it to automatically apply updates and conduct regular scans.
- Always install updates for applications and operating systems when they are available. The longer you delay, the longer you are vulnerable to hackers or malware.
- Use unique, strong passwords that are passphrases for each account (don't duplicate across accounts) and always use two-factor authentication where possible.
- Always backup your data so if your system is compromised, you won't necessarily lose everything. Make sure the backup hard drive is not left connected to your system after you've finished.
- Always practice safe online browsing behaviour and be on the lookout for suspicious links or email attachments.

What to do if you believe you are a victim of hacking

- Run a virus scan to identify and remove any malware.
- Change all your passwords and accounts and notify your financial institution/s.
- Notify your social network to be on alert for any strange links or email attachments.

NATIONAL CYBER SECURITY CENTRE
CSOC
CERT
PAPUA NEW GUINEA

COMMON CYBER THREATS

Visit Our Website for more information: www.ncsc.gov.pg

MALWARE

Malware (short for 'malicious software') is software that cybercriminals use to harm your computer system or network. Cybercriminals can use malware to gain access to your computer without you knowing, in targeted or broad-based attacks.

Malware is the term used to refer to any type of code or program that is used for a malicious purpose.

Cybercriminals use malware for many different reasons but common types of malware are used for stealing your confidential information, holding your computer to ransom or installing other programs without your knowledge.

Protect yourself from malware

Take the following steps to significantly reduce your risk of being affected by malware:

- Use anti-virus software and automatically download signature updates daily.
- Keep all your other software up to date too.
- Use strong passwords and passphrases.
- Backup your files regularly – ideally every day.
- Disable Microsoft Office macros. (Macros are small programs used to automate simple tasks in Microsoft Office documents but can be used maliciously – visit the Microsoft website for information on disabling macros in your version of Office).
- Use safe behaviour online.
- Stay informed on the latest threats
- Regularly check the software installed on your computer, tablet and other devices and uninstall any programs or software that is unused. If you see new programs or software that you did not agree to install, search the program name or ask your local computer repairer or retailer about the program, to see whether it is safe to use.

Prevent malware by installing applications safely

Malware is distributed in several ways:

- By spam email or messages (either as a link or an attachment)
- By malicious websites that attempt to install the malware when you visit, by exploiting weaknesses in your software
- By masquerading as a good application you download and install yourself. Some malware even pretends to be anti-virus or security products.

Protect yourself by only installing the files you need and sourcing them from well known and legitimate app stores.

PHISHING

Phishing is a way that cybercriminals steal confidential information, such as online banking logins, credit card details, business login credentials or passwords/passphrases, by sending fraudulent messages (sometimes called 'lures').

These deceptive messages often pretend to be from a large organisation you trust to make the scam more believable. They can be sent via email, SMS, instant messaging or social media platforms. They often contain a link to a fake website where you are encouraged to enter confidential details.

It doesn't matter if you are an individual using email at home, or what type or size of business you are in, phishing affects everyone.

Protect yourself from phishing attempts

The best way to protect yourself from phishing attempts is to stay abreast of current threats, be cautious online and take steps to block malicious or unwanted messages from reaching you in the first place.

Take the following steps to protect yourself from phishing attempts:

- Don't click on links in emails or messages, or open attachments, from people or organisations you don't know.
- Be especially cautious if messages are very enticing or appealing (they seem too good to be true) or threaten you to make you take a suggested action.
- Before you click a link (in an email or on social media, instant messages, other web pages, or other means), hover over that link to see the actual web address it will take you to (usually shown at the bottom of the browser window). If you do not recognise or trust the address, try searching for relevant key terms in a web browser. This way you can find the article, video or web page without directly clicking on the suspicious link.
- If you're not sure, talk through the suspicious message with a friend or family member, or check its legitimacy by contacting the relevant business or organisation (using contact details sourced from the official company website).
- Use a spam filter to block deceptive messages from even reaching you.
- Understand that your financial institution and other large organisations (such as Amazon, Apple, Facebook, Google, PayPal and others) would never send you a link and ask you to enter your personal or financial details.
- Use safe behaviour online.

RANSOMWARE

Ransomware is a type of malicious software (malware). When it gets into your device, it makes your computer or its files unusable. Cybercriminals use ransomware to deny you access to your files or devices. They then demand you pay them to get back your access.

How does it work?

Ransomware works by locking up or encrypting your files so that you can no longer use or access them. Sometimes it can even stop your devices from working.

The effects of ransomware

Ransomware is a common and dangerous type of malware. It can affect both individuals and organisations.

What to look for

Ransomware can infect your devices in the same way as other malware or a virus. For example:

- visiting unsafe or suspicious websites
- opening emails or files from unknown sources
- clicking on malicious links in email or on social media.

Common signs you may be a victim of ransomware include:

- pop-up messages requesting funds or payment to unlock files.
- you cannot access your devices, or your login doesn't work for unknown reasons.
- files request a password or a code to open or access them.
- files have moved or are not in their usual folders or locations.
- files have unusual file extensions, or their names or icons have changed to something strange.

If any of these things happen to you, check with your friends and colleagues first to see if they made any changes.

Our advice

We recommend you do not pay the ransom. There is no guarantee paying the ransom will fix your devices. It can also make you vulnerable to future attacks. Instead, restore your files from backup and seek advice.

For this reason, it is vital to back up your data and put effective cyber security practices in place.