Online security advice

Documents included

1. Police Assistance Line
2. NSW Police Force – Community Portal
3. How to report Facebook Scams
4. Buy, Swap and Sell Smart
5. NSW Police Force – Protect yourself online
6. NSW Police Force – Protect your debit/credit card
7. NSW Police Force – Protect your identity
8. NSW Police Force – Protect yourself against scammers
9. Know the terms
10. NSW Police Force – How to spot a fake website and not get phished.

Police Assistance Line

Incorporating: Triple Zero (000), 131444, Crime Stoppers NSW and NSW Police Force Customer Assistance Unit.

Mail: PO Box 3427, TUGGERAH NSW 2259 | *Email:* palnet@police.nsw.gov.au | *Fax:* 02 4353 4948

Triple Zero (000)

If you need Police, Fire or Ambulance in an emergency call Triple Zero (000)

When should you call Triple Zero (000)

- If a crime is happening now.
- When a life is threatened.
- When the event is time critical, for example a fire.

What happens if you are speech or hearing impaired?

If you have a speech or hearing disability the triple zero service (000) can be accessed via the National Relay Service on **106**.

Crime Stoppers NSW

24 hour free call: 1800 333 000

Crime Stoppers provides members of the public the ability to report information on criminals and criminal activity anonymously. Information is recorded in Information Reports and transferred to the appropriate Commands. There are rewards of up to $1,000 to members of the public who provide information that leads to an arrest.

www.crimestoppers.com.au

Report Online: www.crimestoppers.com.au
Email: csu@police.nsw.gov.au

Police Assistance Line

24 hour toll free: 131 444

If you are a victim of a crime, other than life threatening or time critical emergency situations, you should contact the NSW Police Assistance Line (PAL).

PAL allows you to report crime over the phone 24 hours a day. Once your report is completed by a customer service representative, your information is immediately available to your local police.

If the crime you wish to report can not be taken over the phone, due to its serious nature, the operator will assist you by advising where you can go to make the report, or by arranging for police to come and see you.

When a police response is required, PAL will arrange for police officers to attend.

PAL can also assist you with general police inquiries.

Contact PAL to report:

- Break and Enter
- Motor Vehicle Theft
- Stealing
- Malicious Damage, including Graffiti
- Minor Motor Vehicle Accidents*
- Lost Property

*You may report a minor vehicle accident if no vehicle has been towed, nobody has been killed or Injured, no driver was under the influence of drugs or alcohol and particulars have been exchanged.

NSW Police Force Customer Assistance Unit

This unit receives and processes written or verbal concerns, complaints and compliments in relation to NSW Police.

FREE CALL **1800 622 571**

Monday to Friday 8am to 4pm
or email to
customerassistance@police.nsw.gov.au

THE COMMUNITY PORTAL EXPLAINED

The Community Portal (https://portal.police.nsw.gov.au) provides access to a range of services including reporting of minor crime and requests for information, all in a secure and confidential online environment. With your details and a valid email address, it's easy to get started. Simply follow our user friendly, interactive form to guide you through the process and if need be, you can save it and come back to it later. Once submitted, you'll receive confirmation that your report has been submitted and you'll receive additional information about what will happen next.

KEY FEATURES

Submit crime reports
Submit non-emergency crime reports to police online.

Apply for information
Request a copy of your police report or other information held by police.

Upload multimedia
Upload a range of multimedia to support your police report.

Update property lists
Add additional property to your existing report.

Email / SMS notifications
Get email and SMS updates about the status of your report.

Help Centre / Live Chat
Visit our Help Centre or chat with one of our representatives.

* Police reports submitted through the NSW Police Force Community Portal undergo a triage process to ensure suitability for reporting online.

Confidential
Confidentiality is key to NSW Police Force operations. Your information is treated with the strictest of confidence.

Always secure
The NSW Police Force Community Portal offers a secure platform for reporting and requesting information.

Easy to use
We value your time so we've made the Portal easy to use across all your modern devices for a seamless experience.

Adds to our existing channels for contacting Police:

Triple Zero (000)
In emergencies or life threatening situations.

Police Assistance Line (131 444)
For non-urgent police assistance and general enquiries.

Crime Stoppers (1800 333 000)
Report information about crime in confidence.

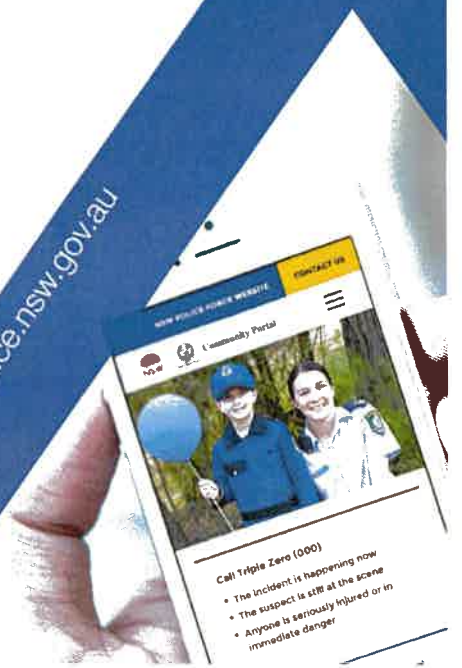
https://portal.police.nsw.gov.au

November 2020 v1.0

NSW Police Force

NSW POLICE FORCE
COMMUNITY PORTAL

https://portal.police.nsw.gov.au



LOST PROPERTY

Losing something you treasure is disheartening and can disrupt your life, especially if you depended on the item you lost. The NSW Police Force can help. With your Community Portal report, you can upload multimedia of your items in a range of formats. So that video of your son's bike, the picture of last year's Christmas toys, can all be uploaded and attached to your report. That way police know exactly what they're looking for.

THEFT

The NSW Police Force is committed to ensuring you have quick access to assistance should theft happen to you. With the Community Portal you can report theft promptly and in detail. The simple and straight forward reporting interface makes it easy for you to enter details logically with the ability to enter multiple items stolen covering every object you could possibly think of. We even give you the ability to save it as a draft and come back to it later.

INTENTIONAL DAMAGE & GRAFFITI

Damage to your property whether by physical damage or by unsightly graffiti causes inconvenience and often involves reporting to insurance companies. Our simple reporting structure not only allows you to report your damage but also provides a Reference Number which can be given to your insurance company. That way you can get the ball rolling straight away.

FAIL TO PAY

For retailers and other businesses, we have provided the ability for you to report incidents when people fail to pay for goods or services that they are able to obtain, prior to paying. Such examples are when a motorist fuels a vehicle up at a service station and then drives off without paying, or when a person leaves a taxi without paying the fare. Reporting is immediate, simple and easy while providing you instant access to a Community Portal Reference Number for insurance claims.

MINOR TRAFFIC CRASH

Minor traffic crashes can occur when you least expect it. Nowadays you can concentrate on organising a tow truck and collecting your belongings. But before making that insurance claim, use the Community Portal to instantly get your Police report reference number. We just need you to know that these reports are only for minor collisions where vehicles are towed and / or there's a minor injury that doesn't require immediate medical assistance. Check out the finer details of this report for more information.

November 2020 v1.0

ACCESS TO INFORMATION

Access to the information the NSW Police Force holds is often requested via various types of applications. Gone are the paper based forms and manual processing and newly announced are the Community Portal's clear, fresh and easy to use online forms. Whether it be requests for police reports, NSW Police Force records or multimedia for an incident your application will be done in minutes all with the required fee, paid seamlessly using our secure, confidential payment facility.

FACEBOOK

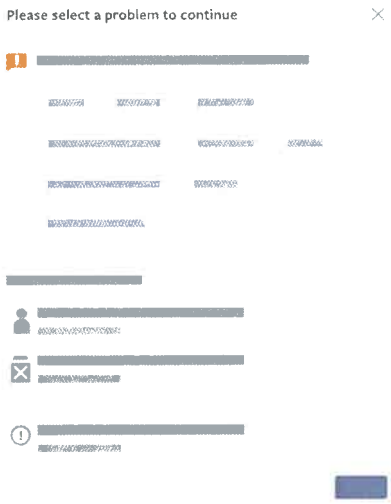
How you can report scams on Facebook services

GUIDANCE FOR AUSTRALIANS

facebook & Messenger

On **Facebook**, you can click on the three dots (...) at the top right of any post, and select 'Find support or report post'.

After that, you can tell us more about why you are reporting, and also access other tools to protect yourself (like blocking a person).



You'll get a response to your report in your support inbox, which is available at facebook.com/support or accessed from the menu within the Facebook app under "Help and Support".

We assess reports against our Community Standards.

If you're ever unsure about how to report something or if you need to provide more context, you can go to facebook.com/report

You can report: profiles; posts; posts on your timeline; photos and videos; messages; Pages; Groups; ads; events; fundraisers; questions; comments; items on Marketplace; or messages that you receive from **Messenger**.

If you would like to report something on Facebook and do not have a Facebook account, visit facebook.com/report to report it to us.

INSTAGRAM

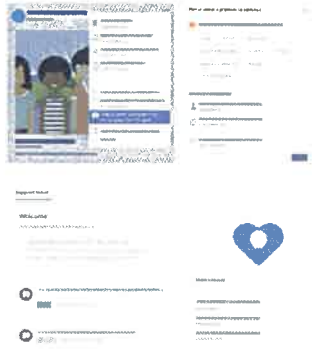
On **Instagram**, you can click on the three dots on the top of any post (...), and select 'Report'.

After that, you can tell us a little more about why you are reporting.

If you can't see the post or would like to provide more context, you can also visit the Instagram Help Centre (help.instagram.com) and follow the prompts to the Privacy and Safety Centre, and then to "Report Something".

WhatsApp

On **WhatsApp**, if you receive a message that you would like to report, click on the name of the contact or group, and scroll to the bottom and click 'Report'.



You can send reports to WhatsApp by contacting us from inside the app.

- On Android:
  Go to WhatsApp >
  tap More options ⋮ >
  Settings > Help > Contact us
- On iPhone:
  Go to WhatsApp >
  Settings ⚙ >
  Help > Contact Us

NSW GOVERNMENT

NSW Police Force

BUY, SWAP AND SELL SMART

Online marketplaces such as Gumtree and Facebook have become a popular place to buy, sell, share, swap and give away unwanted items. While the vast majority of experiences on these sites are successful and hassle-free, online marketplaces are also popular among thieves and scammers. There are a few tips users should follow to ensure they get the best out of their use of these sites:

- **If it sounds too good to be true, then it probably isn't true,** always use common sense. You should inspect the item carefully in person to ensure it is as described in the ad and any issues are known upfront before you exchange any money.
- **Know who you're dealing with.** If you've only ever met someone online or are unsure of the legitimacy of a business, take some time to do a bit more research. It is better to use online sites that you know and trust. Scammers will set up fake online stores or post goods for sale in buyswap-sell groups or online classified sites to trick people into buying items that don't exist.
- For **personal safety** and ease, if possible, you should arrange to meet in a busy public place. Also, it's a good idea to take a family member or friend with you.
- **Never send money to anyone you don't know.** While online transactions can be simple and convenient, please remember that face to face transactions are the best way to minimise the risk of fraudulent activity.
- When buying or selling an item online, **always transact in person, in public, with cash or through payment methods with buyer protection, such as PayPal or Afterpay.**

A MESSAGE FROM NSW POLICE FORCE

BUY, SWAP AND SELL SMART

- A **scheduled payment receipt** is not a confirmation of money transfer, but a notification of a payment scheduled to be made in the future. This can easily be cancelled by the buyer after goods are exchanged.
- **Oops, I paid you too much!** Buyer's will purposely overpay for an item by cheque and request the overpayment be refunded to them by other means, such as cash. The cheque may appear cleared into your account but can be stopped or refused weeks later. Then you've lost the item, the money from the cheque and the amount you refunded to the scammer. Oops!
- A seller claims that there are **brokerage fees, import duties, or other such fees** required to get an item into the country. Do not pay such fees, as you will most often never get the product and will have lost any money you paid.

Car theft

Be aware when selling a vehicle on online there have been instances where a 'buyer' takes the car on a test drive and never returns or, in an accompanied test drive, forces the owner from the car and steals it.
Always sight buyer's identification and record details before allowing a test drive or access to your vehicle. Have a friend or family member accompany you and the buyer on a test drive. Never leave the buyer alone with access to your car.

Delivery Scam via Whatsapp / SMS

If you receive any Whatsapp or SMS messages from potential buyers offering Gumtree or similar delivery as a service, do NOT click on the link or enter your payment details, this is a scam.

Brand name spoofing / phishing

You get an email/SMS that claims to be from Gumtree, Adevinta, Western Union, or another company and offers buyer protection or an online payment system or perhaps a cash prize. Legitimate companies will never send out such emails. Phishing attempts can also come in the form of emails/SMS messages telling you that your account has been disabled, suspended, locked, or something similar and you are asked to click on a link. Do not click on the link.

SMS Scam

An SMS message from a potential buyer asking you to respond by email is most likely a scam. Legitimate buyers and sellers are unlikely to want to be emailed if they are already texting you.

For more information on how you can protect yourself online, visit the Australian Government's online safety section **https://info.australia.gov.au/information-and-services/public-safety-and-law/online-safety**

or SCAMWATCH online shopping scams **https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams**

NSW GOVERNMENT

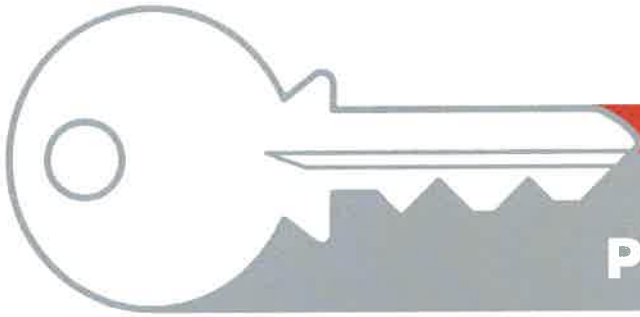
NSW Police Force

000 **Triple Zero (000)** For emergencies or life threatening situations

Police Assistance Line (131 444) For non emergencies

CRIME STOPPERS **Crime Stoppers (1800 333 000)** To provide crime information, it can be in confidence.

Follow us on [illegible] or visit [illegible]



NSW POLICE FORCE CRIME PREVENTION SERIES

Protect yourself online

Protect yourself from fraud

The everyday use of mobile telephones, tablets and personal computers is now common place in most people's lives. We use these devices to verbally and visually communicate, for business, for financial transactions and as multipurpose storage devices which we are now even more reliant upon.

These devices hold key information that can be targeted in several ways including; scam emails, false representation of a service provider, inadequate software protection or password security.

These are just some methods used by criminals to obtain your personal details and those of your family which can lead to the theft of your identity. Here are some simple steps we can all take to help protect ourselves against this type of crime.

Protect your password

- **DON'T** use the same password for all your devices or access systems.
- **DON'T** use names or words easily linked to you (eg; family, pet or school names) in your password.
- **CHANGE** your password regularly.
- **DON'T** GIVE YOUR PASSWORD TO ANYONE.

Protect your computer or mobile device

- **INSTALL** reliable anti-virus protection for all your computers and mobile devices.
- **UPDATE** your anti-virus protection regularly.
- **DISABLE** unwanted applications - if you don't use it, lose it.

Protect your identification online

- **DON'T** let anybody else access your personal information or your devices.
- **DON'T** give anyone remote access to your devices.
- **DON'T** access emails senders you don't know.
- **DON'T** share your personal or financial information online such as driver's licence details, date of birth, etc.

If you believe you have been a victim to a cyber related offence – report it immediately on **www.acorn.gov.au**

For more crime prevention information visit us on ***www.police.nsw.gov.au***

NSW Police Force

NSW GOVERNMENT Justice

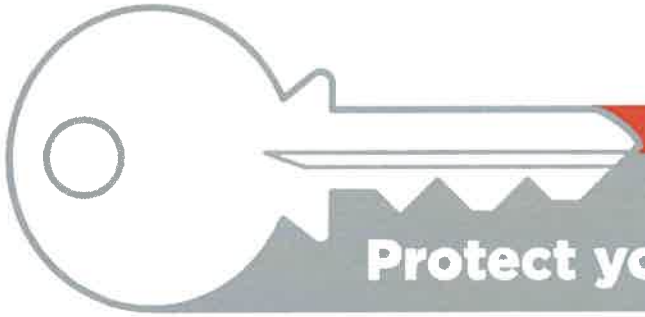
policebank member owned banking

Westpac

Triple Zero (000) For emergencies or life threatening situations.

Police Assistance Line (131 444) For non emergencies.

Crime Stoppers (1800 333 000) To provide crime information. It can be anonymous.



NSW POLICE FORCE CRIME PREVENTION SERIES

Protect your debit/credit cards

Protect yourself from fraud

As we move towards a cashless society, the use of debit and credit cards over cash is common place.

Your cards hold highly personal information that, if not safeguarded, can be copied or stolen. This could allow criminals to access your funds or identification.

Here are some simple steps we can all take to help protect our card information from this type of crime.

Protect your card

- **DON'T** lose sight of your debit and credit cards.
- **INSIST** the transaction be done in front of you.

Protect your PIN

- **DON'T** share your PIN with anyone.
- **COVER** your hand when entering your PIN.
- **CHANGE** your PIN regularly.

Protect your account

- **REQUEST** registered mail or pick up from the branch for replacement cards and PIN information.
- **SECURELY** dispose of banking information, bills and expired/unwanted cards preferably by shredding all documents.
- **ALWAYS** check your financial statements against your purchases. If you see something that doesn't look right, contact your financial institution immediately.

Protect your card online

- **USE** recommended electronic payment enablers when buying online.
- **INSTALL** and maintain anti-virus/anti-malware software on your devices.

If you believe you have been a victim to a cyber related offence – report it immediately on **www.acorn.gov.au**

For more crime prevention information visit us on ***www.police.nsw.gov.au***

NSW Police Force

NSW GOVERNMENT Justice

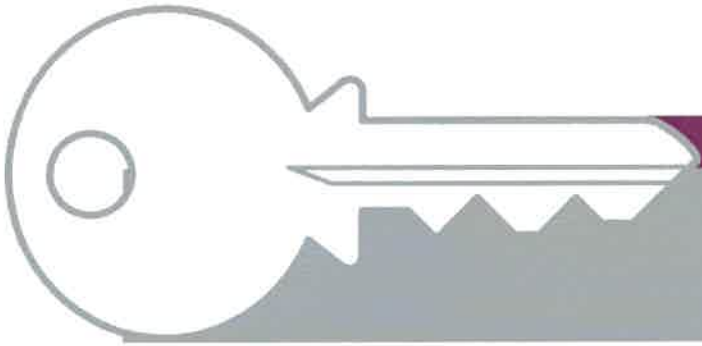
policebank

Westpac

Triple Zero (000)
For emergencies or life threatening situations.

Police Assistance Line (131 444)
For non emergencies.

Crime Stoppers (1800 333 000)
To provide crime information. It can be anonymous.



NSW POLICE FORCE CRIME PREVENTION SERIES

Protect your identity

Mail Theft

Modern life is all about easy access and convenience for the customer. This includes how we receive and send goods and information.

Items such as credit cards, drivers licences and utility statements sent out in the mail include vital personal details of you and your family.

In the wrong hands some of this information can be used to create false identifications and used for crime. This type of crime costs millions of dollars each year and can have devastating consequences for your financial reputation.

By following some of these simple tips **we all** can better protect ourselves from this type of crime.

Secure your mail

- Always install a lockable mailbox.
- Always use a quality lock on your mailbox.
- Never allow your mailbox to become full or overflow.

Protect your mail

- Always arrange to collect new credit cards from the bank or post office.
- Always have mail held at the post office or collected by a friend when you're away for extended periods.
- Always have your mail cleared daily.

Protect your identity

- Always beware of 'cold calling' and confirm who you are talking to.
- Never give any of your personal details to people you don't know or trust.
- Always contact your bank, financial institution or service provider if you think you have been contacted by a scammer.

If you are aware of mail being stolen and used to obtain fraudulent identity, please contact Crime Stoppers on 1800 333 000 or online at ***www.crimestoppers.com.au***

For more crime prevention information visit us on ***www.police.nsw.gov.au***

NSW Police Force

NSW GOVERNMENT Justice

MailSafe
A failsafe against mail theft.

Triple Zero (000)
For emergencies or life threatening situations.

Police Assistance Line (131 444)
For non emergencies.

Crime Stoppers (1800 333 000)
To provide crime information. It can be anonymous.

NSW POLICE FORCE CRIME PREVENTION SERIES

Protect yourself against scammers

Protect yourself from fraud

With the advances in electronic communication, criminals don't necessarily need to be face to face to steal from you. Scams are constantly evolving and scammers can go to great lengths to cause people to part with money or information.

Scammers may pretend to be from your bank or a service provider, offer sports betting or short term investment opportunities. They can claim the ability to return owed monies from overseas, often romance and dating opportunities plus numerous other approaches. On the surface these **may** appear to be genuine.

Here are some simple steps to help protect yourself against scammers.

If it sounds too good to be true . . .

- **NEVER** send money or give credit card or online account details to anyone you don't know and trust.
- **ALWAYS** seek independent financial and/or legal advice before making any investment or purchasing decisions.
- **NEVER** rely solely on advice from the person trying to sell you the service or investment.

Door to door sales or 'Tradie scams'

- **DON'T** be pressured into signing or paying up front.
- **ALWAYS** research a company or service provider prior to paying or agreeing to a contract.
- **ALWAYS** read any contract or service paperwork carefully prior to paying for any work.

Protect your personal information

- **NEVER** give your personal or bank account details to people you don't know and trust.
- **ALWAYS** contact your bank, financial institution or service provider if you have been contacted by a scammer.
- **DON'T** use the numbers provided on the email to confirm an email's legitimacy before replying.

Don't take things on face value

- **DON'T** be fooled by an email that looks legitimate or appears to link to a genuine website.
- **DON'T** open suspicious or unsolicited emails (spam) – ignore them.
- **ALWAYS** beware of 'Cold Calling' and confirm who you are actually talking to.

If you believe you have been a victim to a cyber related offence – report it immediately on **www.acorn.gov.au**

For more crime prevention information visit us on ***www.police.nsw.gov.au***

NSW Police Force

NSW GOVERNMENT Justice

policebank member owned banking

Westpac

Triple Zero (000) For emergencies or life threatening situations.

Police Assistance Line (131 444) For non emergencies.

Crime Stoppers (1800 333 000) To provide crime information. It can be anonymous.

KNOW THE TERMS

App - Software which allows its user to perform tasks. For example, Microsoft Word. Phones and tablets also have apps, including Facebook and weather apps.

Bot - A bot is a computer that has been compromised by malicious code. This can sometimes happen without people knowing their computer has been infected. 'Bots' can sometimes work together in something called a botnet, a network of compromised computers that send out malicious software. Unfortunately, due to the number of computers involved it is sometimes hard to trace the culprit.

Brute force attack - The attempt to gain access to a computer resource using repeated guesses at passwords until it gets the right ones.

Catfishing - Catfishing is where someone sets up a fake online identity to lure people into emotional relationships. This can often be used to leverage that person's trust and gain personal information for the purpose of identity fraud or theft.

Cloud computing - A cloud allows people to store and access saved content over the internet, instead of on a hard drive. For example, iCloud. Cloud computing also encompasses the delivery of services and resources over the internet such as access to applications and infrastructure.

Cookie - A piece of code or data created by a web browser (web server), which is stored on a person's computer and can identify the user and customise web pages.

Cyber-attack - A cyber-attack is a deliberate attempt to access an information computer system, usually with the goal of theft, disruption, damage or other unlawful actions.

Darknet - A hidden 'neighbourhood' of the internet, which is only accessible using non-standard protocol. It is basically a marketplace for illegal substances, such as software or illegal images or videos.

Distributed Denial of Services attack (DDoS) - A DDoS attack happens when multiple computer hosts send requests to a target website at such a rate that it crashes.

Encryption - Encryption is the process of converting data into an unrecognisable form. This means the data is not easily understood by unauthorised party.

Firewall - A Firewall is a barrier which protects computers and networks from unauthorised access.

Malware (malicious software) - Malware is intrusion software. It includes computer viruses, worms, trojan horses, ransomware, spyware, adware and scareware.

KNOW THE TERMS

 **Money mule** - A person who receives and transfers illegally acquired money on behalf of others. Unknowing mules can be recruited through online scams.

 **Phishing -** Phishing attacks use fake emails and fake websites designed to fool recipients into divulging personal financial information such as credit card numbers, bank account details, and usernames or passwords.

 **Ransomware** - Ransomware sneaks into your computer, usually via a website or document, and then locks or encrypts your computer and scams you into paying a ransom to unlock it again.

 **Remote Access Tool (RAT) -** A tool that allows someone to access a computer from a remote location.

 **Scams -** Schemes that seek to take advantage of people to gain a benefit, such as money or personal information.

 **Secure Sockets Layer (SSL, or the 's' in https) -** A barrier that allows internet users to send encrypted messages. This is mostly used with online shopping or banking. A web address that has an 's' after http indicates that an SSL connection is in use.

Spam - Unsolicited emails sent, often sent for the purposes of marketing.

 **Spear phishing -** A targeted phishing attack, which usually contains personal information about the person who receives the email.

 **Virus -** A virus is a piece of programming code which is contained within another program. It causes damage by infecting the computer or device with the virus. Viruses can erase data or damage content on your computer or device.

 **Watering—hole** - A compromised website which contains malware that is intended to compromise visiting users.

 **Whaling -** A targeted phishing attack, targeted at senior executives of companies.

NSW Police Force

How to Spot a Fake Website and Not Get Phished

If there's one thing that cybercriminals excel at, it's instilling a false sense of trust by taking advantage of our familiarity with current events and playing off mental triggers, such as our feelings of sympathy. We call this "social engineering," and it's a key trait in one of the most popular online scams: phishing emails that link to fake websites.

What is Phishing?

Phishing is a form of Internet fraud where a scammer, pretending to be a legitimate person or organization, sends you an email that tries to trick you into revealing personal or financial information, such as credit card numbers, social security numbers, and passwords. Phishing is one of the most common scams on the web and cybercriminals are constantly modifying their attacks to include details that will make the recipient believe the scam is real.

In a phishing attempt, a cybercriminal may send you a message purportedly from your bank, asking you to confirm your account information by clicking on a link. Once you click on the link, it launches a Trojan (a malicious program that appears to be benign) that installs a keystroke logger on your machine. This keystroke logger then captures everything you type, including passwords.

The link may also take you to a fake bank website that asks you to enter your personal information. To the untrained eye, the fake site looks identical to the bank's real homepage because the scammer has copied files from the real site. However, when you attempt to log in to your account, the site asks for information that the real site never would. It may ask not only for your name and address, but also your account number, password, the last eight digits of your debit card number, and your ATM PIN.

Another common phishing trick that hackers use is erecting fake sites at commonly misspelled addresses in the hope of catching unsuspecting web surfers. Mistyping a webpage address can lead you to these fake sites, an occurrence that's not uncommon for people who regularly surf the Internet. Creating fake sites is called typo-squatting, and like most cyber tricks it's designed to get your information and your money.

Recognizing Phishing and Fake Websites

The good news is that you can avoid scams by looking for tell-tale signs that indicate when a site is fake, or an email is phishy. The next time you are not completely confident that you are on a legitimate website or that an email you received is valid, check for these signs:

1) Uses an incorrect URL—If you are used to going to your bank via a regular address and the address of the site you land at is not the same name, you can be confident that you are not at the real site. Always double check to make sure that the site address is accurate. You can also hover your mouse pointer over a link in the email to verify that the link is directed to the same site that the email came from.

2) Asks for banking information—A real bank would never ask for your bank account information or your debit card and PIN numbers via email. Be wary of any email or site that asks for sensitive information (such as your Medicare number or Passport number) that is beyond your standard login.

3) Uses a public Internet account—Before you click on any link sent to you by email, take a look at the sender's email address. If the email is from a public account but claims to be from your bank or other business, do not trust the email. Moreover, do not trust any email or website that asks you to "confirm" sensitive account information, because this is surely a scam. You should also make sure that any email claiming to be from your bank includes your given name in the message, such as "Dear William Smith," instead of "Dear Valued Customer." Real banks address messages to you by name as a way of confirming your relationship.

4) Includes misspelled words—If a bank asks you to log in to your "account," this is pretty good clue that you've stumbled upon a phishing email or fake website. Real companies have staff checking the accuracy of emails and website, and a mistake like this would be caught before it was sent or published. If you see a misspelling or a misuse of the company name, look for other mistakes and clues to confirm your suspicions—and don't enter any of your personal information on the site.

5) Is not a secure site—Legitimate e-commerce sites use encryption, or scrambling, to help insure that your payment information remains safe. You can see if a site uses encryption by looking for a lock symbol in the browser window. Clicking on the lock symbol allows you to verify that a security certificate was issued to that site, a sign that it's a legitimate, trusted website. You should also check that the address starts with "https://" rather than just "http://". Do not enter payment information on any site that isn't secure.

Northern Beaches Police Area Command
Corner of Fisher Road and St David's Avenue
Dee Why 2099
T 02 9971 3399 F 02 9971 3375 W www.police.nsw.gov.au
TTY 02 9211 3776 for the hearing and speech impaired ABN 43 408 613 180

NSW Police Force

6) Displays low resolution images—Scammers usually erect fake sites quickly, and this shows in the quality of the sites. If the logo or text appears in poor resolution, this is an important clue that the site could be phony.

Protecting Yourself

While these tips will go a long way in helping you identify phishing and fake sites, keep in mind that the scammers are always looking for ways to up their game and make their scams more convincing. It helps to be aware of the mental shortcuts you use and to really take the time to ask yourself if the site seems legitimate. Here are some ways in which you can avoid being caught in a cybercriminal's net:

1) Educate yourself—Read up on the latest scams so you know what to lookout for. And be familiar with what a phish looks like so you can recognize common tricks when you see them.

2) Use common sense—Read your emails carefully, checking to make sure you know the sender, and be suspicious of any email that asks for your personal or financial information. Also, be very cautious when downloading any attachments or files from an email, unless you know and trust the sender.

3) Practice smart surfing—When on the web, make sure that the website you're visiting is secure before you enter any information. If you have any doubts, enter a fake password, since phony sites will accept false information. To better protect yourself, you may also want to use a search engine to help you navigate since they can catch misspellings and prevent you from landing on fake websites. There are searching tools that some security software companies offer which indicates in your search results whether sites are safe or not.

4) Use technology to protect you—Comprehensive security software with anti-phishing technologies, can help protect you. Just make sure that your software is up to date with the latest security protections by enabling automatic updates or clicking the "update" button on your security software program.

5) Be vigilant all the time—You also want to take precautions when you're offline, such as monitoring your bank and credit card statements for any suspicious charges or transfers. And consider changing your passwords regularly. Make sure you create strong passwords that use a combination of letters, numbers, and special characters, and that don't use nicknames, birthdays, or other information that other people may know.

6) Report anything you think is suspicious—If you do come across what looks to be a phishing attempt, help yourself and others by reporting it.

There are also numerous websites which offer plenty of information in relation to protecting yourself against scams. These are:

https://www.scamwatch.gov.au/

https://www.cyber.gov.au/report

https://www.police.nsw.gov.au/crime/frauds_and_scams

https://nsw.crimestoppers.com.au/fraud-and-id-theft/

http://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity

eyewatch Find your local police on Facebook
www.facebook.com/NorthernBeachesPAC

Like us on Facebook

Northern Beaches Police Area Command
Corner of Fisher Road and St David's Avenue,
Dee Why 2099
T 02 9971 3399 **F** 02 9971 3375 **W** www.police.nsw.gov.au
TTY 02 9211 3776 for the hearing and speech impaired ABN 43 408 613 180