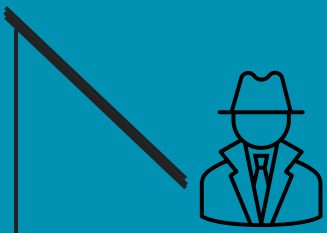
TechSafe
Business Cyber Security

Be a Smart Phish

Phone and Text Scam Awareness Booklet by TechSafe

(Phishing is the act of using fake messages to steal your information)



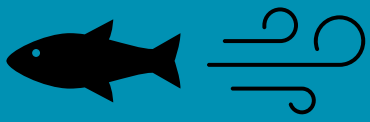
In Confidence

Common Scammer Tactics



Sense of Urgency

Scammers want you to act without thinking to increase your chances of falling for their scam. Always slow down when receiving messages.





Trusted Actors

Scammers often pose as banks, IT Support, family members or other trusted figures to gain your trust.

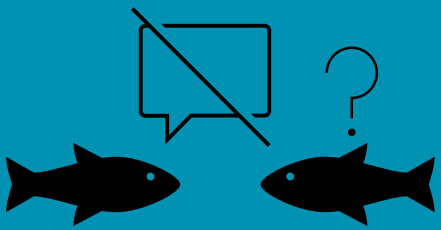
TechSafe
Business Cyber Security



Odd Requests

Scammers want your money and information, so will likely try and get it. Theses often include links, downloads, or fake helplines, so be suspicious when an unknown number sends you one of these.



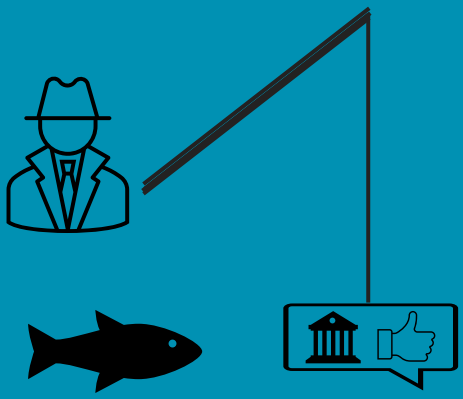




Air of Secrecy

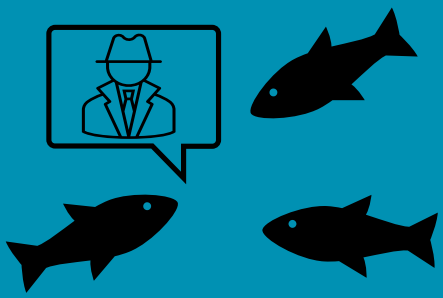
Longer term scams will try and swear you to secrecy to prevent friends and family from helping to recognize the scam.

When a Message or call is Suspicious



Don’t Trust it

Scammers will attempt to convince you of their legitimacy, and if you listen to them, they can be quite convincing. Always stay alert, regardless of what the suspicious messenger tells you.



Discuss it

Talking about an odd message you received will let others pool their knowledge with yours. This makes it much easier to detect scams and raises both your and their phishing awareness.

TechSafe
Business Cyber Security





Talk to the Real Version

Switch to the official / normal number of the organization or person that contacted you. This doesn't let scammers have any chance of success. If the exchange was real, they will be able to continue where you left off.

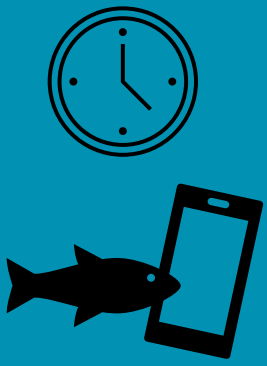




Report it

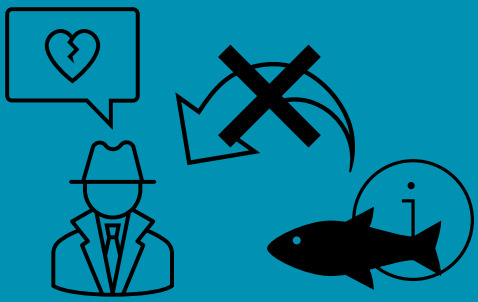
Report the scammer to the National Cybersecurity Center to help prevent others from falling for it.

Good Anti-Phishing Practice



Slow Down

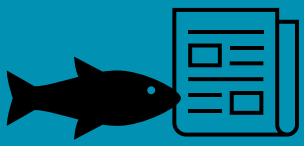
When you receive an unexpected message from a number you don't recognize, wait a few minutes before acting after reading it. This'll ensure you've thought the message through before continuing.



Keep Private Info Private

Avoid giving out personal information over the phone, through messages, or through any link you received from a number your unfamiliar with.

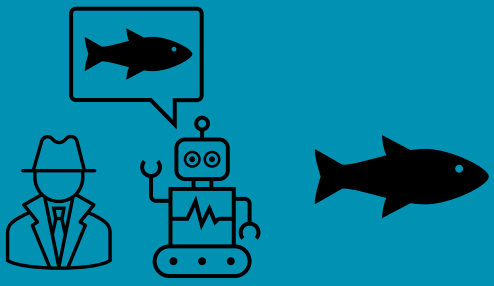
TechSafe
Business Cyber Security



Keep Up-to-Date on Scam News

Knowing about scams before they arrive will make you much less likely to fall for them.

It will also make you more scam aware in general, so even new scams will be unlikely to trip you up.



Don’t Assume it’s Not a Scam

Modern phishing can accurately recreate family voices and replicate service emails with perfect grammar and spelling. Don’t rely on looking for poor grammar and spelling, accents, or other similar tells.

Contact Info and Help Lines

- These are the phone numbers and official websites of some organization's scammers may pretend to be.

ANZ:
Phone: 0800 269 296
Website: anz.co.nz

ASB:
Phone: 0800 272 372
Website: asb.co.nz

BNZ:
Phone: 0800 735 901
Website: bnz.co.nz

Westpac:
Phone: 0800 400 600
Website: westpac.co.nz

Kiwibank:
Phone: 0800 113 355
Website: kiwibank.co.nz

Ministry of Immigration:
Phone: 0508 558 855
Website: immigration.govt.nz

Inland Revenue:
Phone: 0800 257 777
Website: ird.govt.nz

Police:
Phone: 105
Website: police.govt.nz

NZ Post:
Phone: +64 9 977 0102
Website: nzpost.co.nz

Amazon:
Phone: Call from website.
Website: www.amazon.com

Report scams to the National Cybersecurity Center at:
www.ncsc.govt.nz/report/business-and-individuals/

For scam related news and more information about phishing:
ownyouronline.govt.nz

TechSafe
Business Cyber Security

Be a Smart Phish

Practical Steps to Take After a Scam Booklet by TechSafe

(Phishing is the act of using fake messages to steal your information)



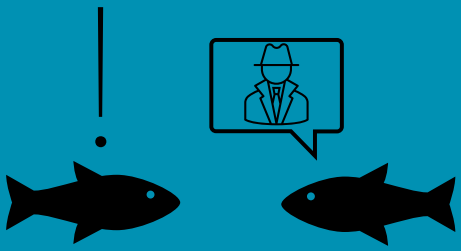
In Confidence

Signs You've Been Scammed



Strange Account Access

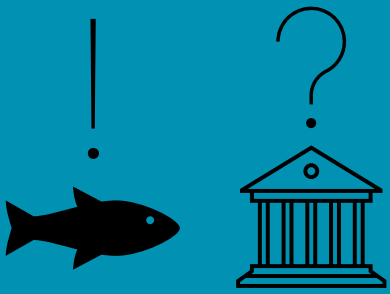
If you recently received an unprompted call or text message where you provided sensitive information, such as passwords or bank details, and the affected accounts have later been accessed by others, you may have been scammed.



Similar Messages

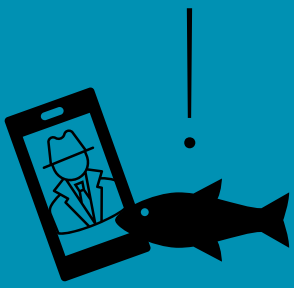
If you engage with an unprompted call or text message, and you or others receive similar messages afterwards, you may have been scammed.

TechSafe
Business Cyber Security



Inconsistent Details

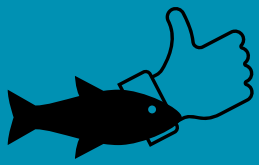
If after engaging with an unexpected call or text message you later find out that some of the details of the conversation were untrue, such as a family member not really switching phone numbers, you may have been scammed.



Recognizing Phishing Tactics

If your knowledge on how scammers conduct phishing has improved, you may recognize phishing tactics in old messages. If this happens, you may have been scammed.

After You've Been Scammed



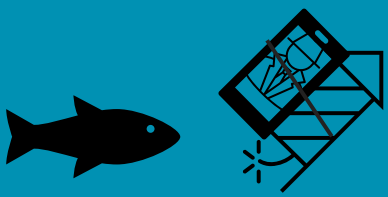
First: Calm Down

Scammers can be very convincing, especially when they are able to learn about you beforehand. There's nothing to be ashamed about over falling for a scam, what's important is taking the appropriate action afterwards.

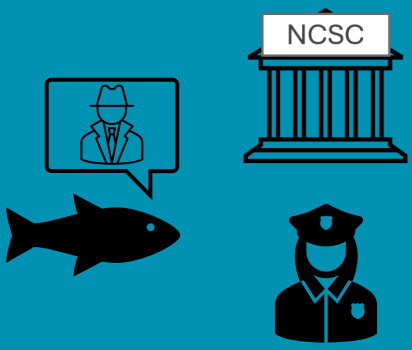


Second: Disconnect

stop all contact with the scammers immediately. Further contact only means further risk.



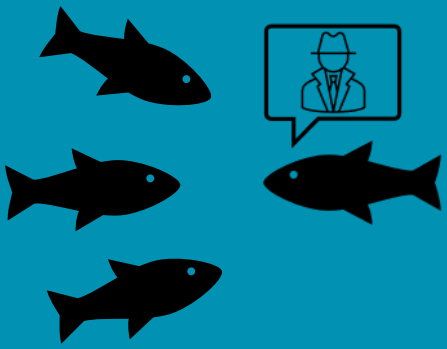
TechSafe
Business Cyber Security



Third: Report

Report the scam to the National Cybersecurity Center to help others avoid the scam.

If you lost any money or property because of the scam, call your bank to see if they can halt or reverse the payment. Then, notify the police on 105 about the scam.



Finally: Discuss

Discussing the scam with friends and family will raise scam awareness in your community and help you move past this unfortunate incident.

Useful Resources

- See TechSafe's phishing awareness booklet for more information on scam awareness.

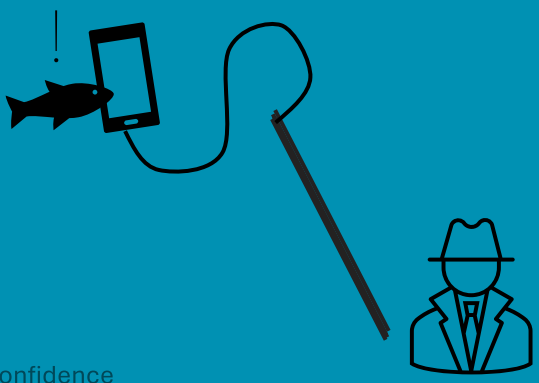
Report scams to the National Cybersecurity Center at:
www.ncsc.govt.nz/report/business-and-individuals/
For scam related news and more information about phishing:
ownyouronline.govt.nz

TechSafe
Business Cyber Security

Be a Smart Phish

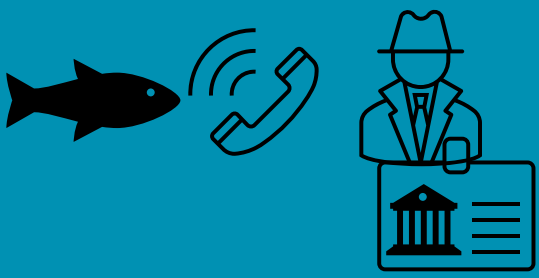
Dealing with Phone Scams Booklet by TechSafe

(Phishing is the act of using fake messages to steal your information)



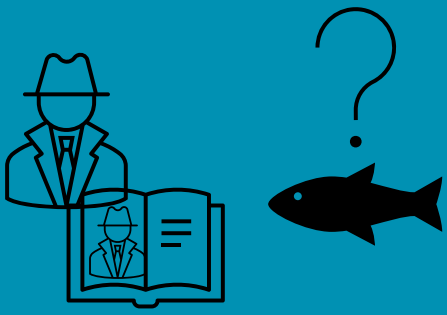
In Confidence

When you Receive a Random Call...



Be Cautious

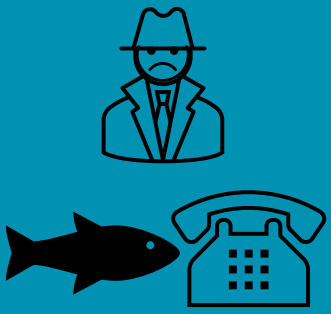
Always be suspicious if someone claiming to be from government agencies, businesses or other organizations randomly calls you. It's very rare for this to happen. Don't give up any personal information or money on any call like this.



Look for Common Scam Tactics

Phone scammers will employ many of the same tactics as other scammers, such as inspiring urgency and swearing you to secrecy. If you notice these signs, it may be a scam.

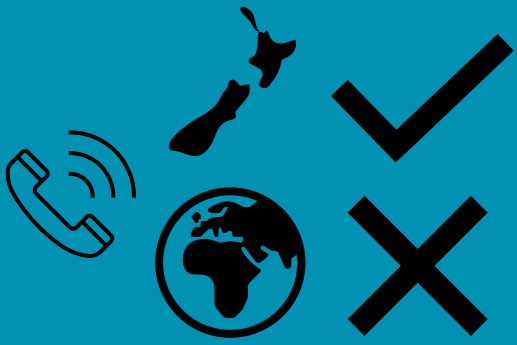
TechSafe
Business Cyber Security



Don’t be Afraid to Call Back

Whoever is calling you will be able to pick up where you left off after you call them back. Make sure to use the official number on their website over one the caller provides.

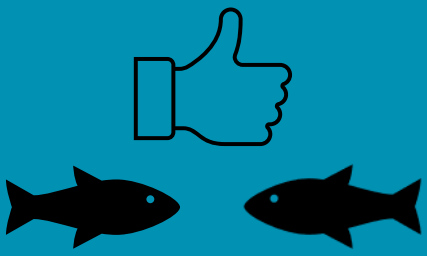
If a call center needs to call you, they will be understanding if you’re suspicious.



Check the Phone Number

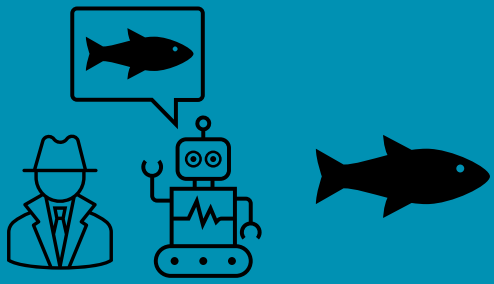
Phone scammers may be unable to use a phone number from New Zealand, which is represented by a ‘+64’ at the start. Treat any number without this with caution.

Good Phone Phishing Awareness Techniques



Verify Before Sharing

If you receive a phone call from someone on an unfamiliar number, don't share or do anything until you're sure they are who they claim to be.



Know that it Could be Fake

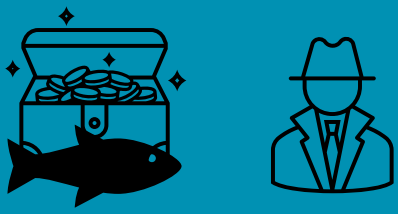
Modern scammers are very good at accurately replicating the voices of family members and have perfect grammar with local accents.

TechSafe
Business Cyber Security



Know What Won't be Asked

No one on the phone should ever ask for your passwords or sensitive personal information like passport details. Never give these details out over the phone.



Hold onto Your Money

Be cautious when dealing with money transfers over the phone. Organizations and family members should never try to get money from you this way, and you should try and get in person confirmation from family members.

Contact Info and Help Lines

- See TechSafe's Phishing Awareness Booklet for more information about phishing.
- These are the phone numbers and official websites of some organization's scammers may pretend to be.

ANZ:
Phone: 0800 269 296
Website: anz.co.nz

ASB:
Phone: 0800 272 372
Website: asb.co.nz

BNZ:
Phone: 0800 735 901
Website: bnz.co.nz

Westpac:
Phone: 0800 400 600
Website: westpac.co.nz

Kiwibank:
Phone: 0800 113 355
Website: kiwibank.co.nz

Ministry of Immigration:
Phone: 0508 558 855
Website: immigration.govt.nz

Inland Revenue:
Phone: 0800 257 777
Website: ird.govt.nz

Police:
Phone: 105
Website: police.govt.nz

Report scams to the National Cybersecurity Center at:
www.ncsc.govt.nz/report/business-and-individuals/

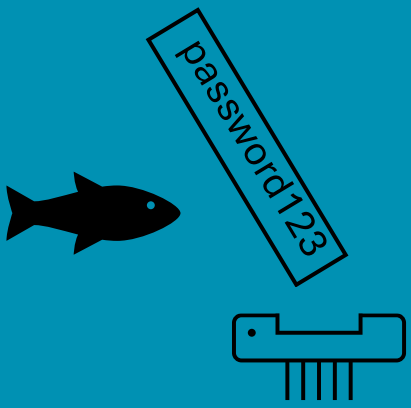
For scam related news and more information about phishing:
ownyouronline.govt.nz

TechSafe
Business Cyber Security

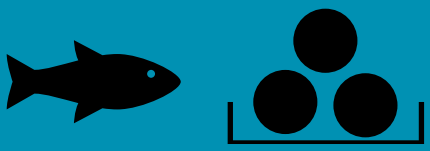
Be a Smart Phish

Good Password Policy Booklet by TechSafe

(Passwords are secrets used to access user accounts)



Creating Strong Passwords



Add Some Extra Characters

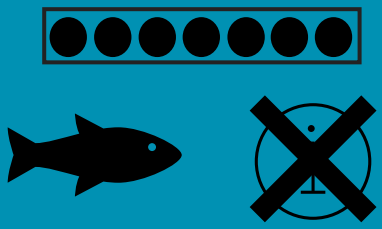
Longer passwords are more difficult for both machines and people to guess. An extra couple characters can be the difference between an attacker being able to figure out your password after a few hours or a few centuries.



Choose Varied Characters

Using a mix of upper and lowercase letters, numbers and special characters (like !, ? or @) will make it more difficult for an attacker to guess your password.

TechSafe
Business Cyber Security



Make it Abstract

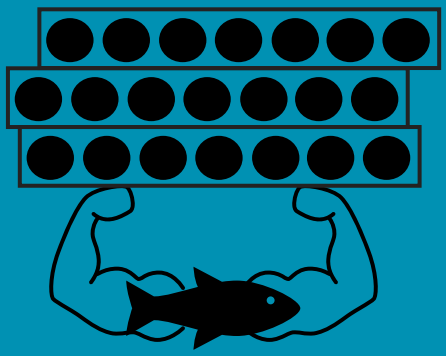
Your password shouldn't be something which holds other meaning for you. For example, your mother's maiden name. If an attacker learns this information about you, it will make your password much weaker.



Use a Passphrase

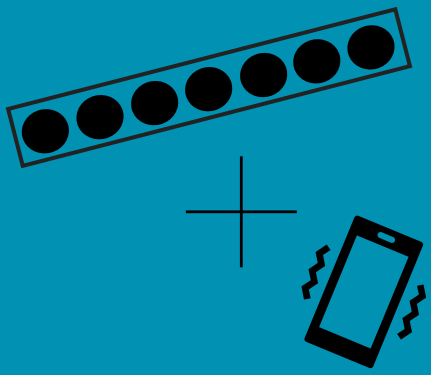
If you struggle to remember a strong password, try a passphrase. Passphrases are a series of random words, such as 'HillWindowElephant' (don't use that one). Passphrases are easier to remember than passwords, while remaining long enough to be secure.

Good Password Practice



Keep Passwords Unique

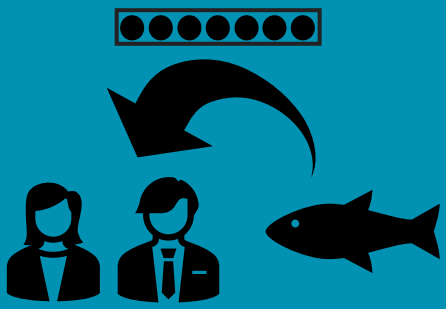
Using different passwords is essential, as when using the same password an attacker who knows your password for one account can simply try the same password on all your accounts.



Use Multi-Factor Authentication

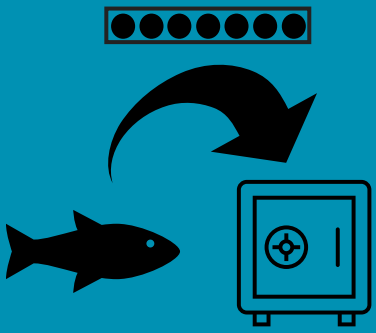
Multi-factor authentication, or MFA as it is sometimes referred to, protects your accounts by requiring a second layer of authentication, such as a code sent to you by text.

TechSafe
Business Cyber Security



Use a Password Manager

Most modern browsers have built-in password managers which can automatically generate, remember and fill in passwords. Using these is an easy way to remember many unique, strong passwords.



Never Give Away Your Password

You should always keep your password secret. If someone knows your password, there may be little stopping them from accessing your accounts.

Useful Resources

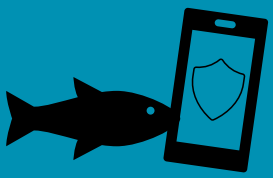
- For more information about creating strong passwords, using password managers, and more, see:

www.ownyouronline.govt.nz/how-exposed-am-i/

TechSafe
Business Cyber Security

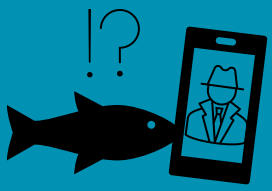
Be a Smart Phish

Smartphone Safety Booklet by TechSafe



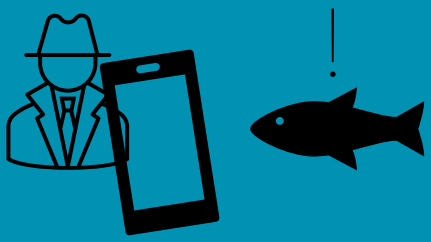
In Confidence

Recognizing Malicious Apps



Always Be Alert

Malicious actors can register apps on common app stores designed to steal your personal information or take control of your device. Always think before you download.



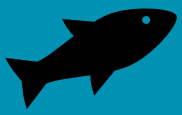
Check Who Made It

Check who released the app onto the app store. Make sure it's who you expect. Also try and stick to apps made by accountable distributors, such as businesses.

In Confidence

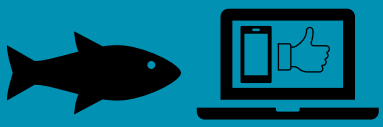
TechSafe
Business Cyber Security





Check the Downloads and Reviews

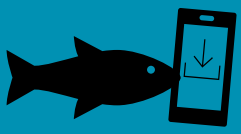
Make sure to check how many people have downloaded the app and read a few reviews. Few downloads or reviews, generic reviews (suggesting they may be fake), or reviews calling the app a scam or a virus are all signs an app may be malicious.



When in Doubt, Look it Up

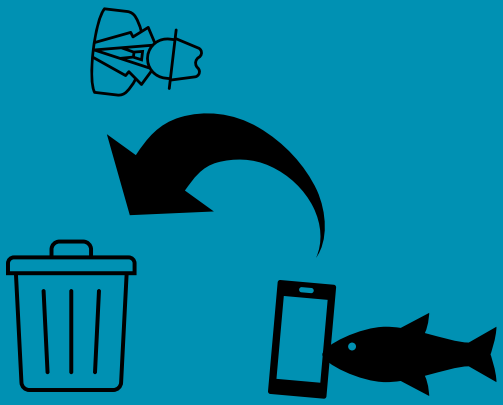
If you want to download an app, but you're not sure if it's safe, Google the app's name as well as its distributor. If the app is real, there will be results confirming the apps legitimacy.

General Phone Safety



Update your Phone

Both the apps on your phone and the phone itself are constantly changing, not only with the addition of new features, but new discovery of new security issues as well. Keeping on top of new fixes keeps security flaws out of your phone.

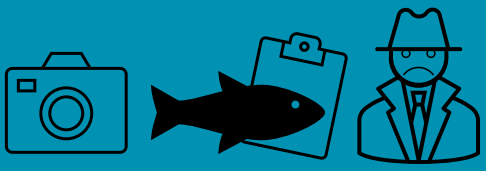


Delete Apps you No Longer Use

Deleting apps when you no longer need them keeps the number of possible ways your information could be stolen down.

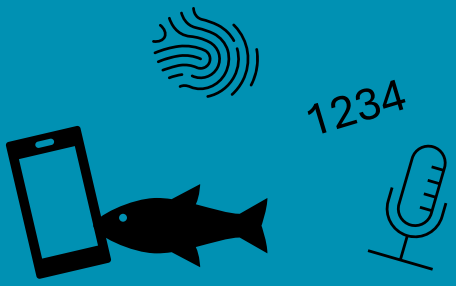
TechSafe
Business Cyber Security

Not on the List, Bud



Think Before Giving Permissions

Malicious apps may try to gain access to your personal information by requesting access with a prompt. When you receive such a prompt, think if the app doing the request really needs the requested permissions. If you're unsure, deny them.



Use Secure Sign In Methods

Short pins, some biometrics (fingerprints, face scan, etc.), and other simple authentication methods are often easy to guess or simple to forge. Especially in the age of artificial intelligence, it's better to rely on stronger methods like passwords.

Useful Resources

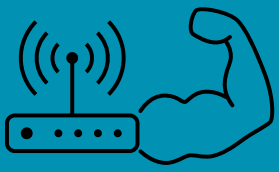
- To learn how to deal with an unknown caller, see the TechSafe phone scams booklet.
- For more information on passwords, see the TechSafe good password policies booklet.

TechSafe
Business Cyber Security

Be a Smart Phish

Network Safety Booklet by TechSafe

(Network refers to something that allows a device to connect to the internet, such as Wi-Fi or Ethernet)



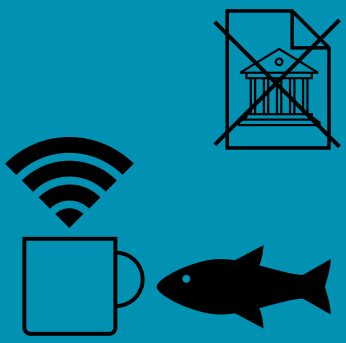
In Confidence

When Using Public Networks



Avoid Logging in Where Possible

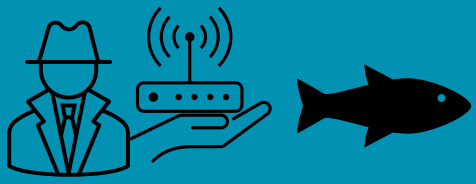
On public networks, anything you do on the internet is visible to any other device on the same network. This means if you login to anything, a malicious actor may be able to intercept your details.



Don't Access Anything Important

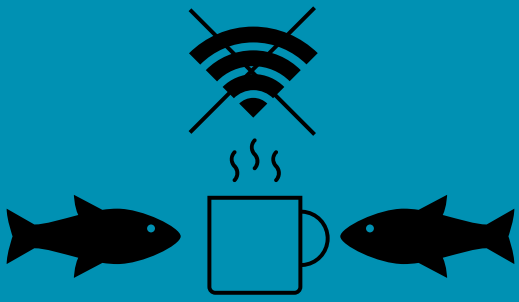
Anything you access on a public network can be seen by others on the same network. You shouldn't access important items on them, includeing bank details, email accounts, etc.

TechSafe
Business Cyber Security



Check the Name

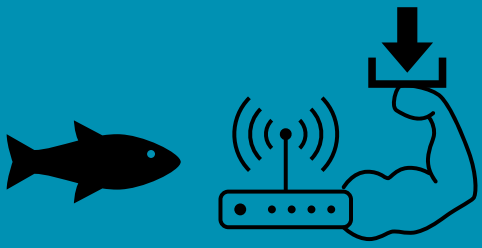
Make sure that you connect to the correct network when trying to use public Wi-Fi. This includes checking for subtle typos in the name. A malicious actor may register a network with a similar name to try and steal your information.



Avoid Connecting

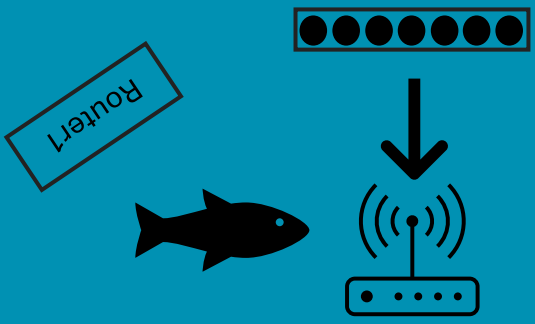
The simplest way to avoid issues with public Wi-Fi is to avoid connecting entirely. Only connect to public Wi-Fi when you want to use it.

When Using a Private Network



Keep Your Router Updated

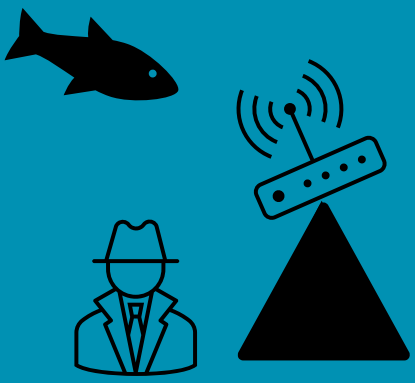
Make sure that your router is set to update automatically. Keeping your router updated is the best way to keep it secure against attack.



Change Your Router's Password

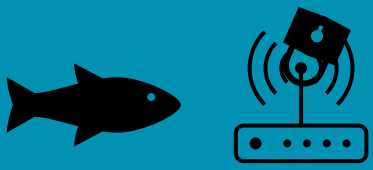
The default password for most routers is publicly available on the internet. Changing the password is essential to guarantee router security.

TechSafe
Business Cyber Security



Make Sure Your Router is Supported

Routers only receive updates for so long after their release. If your router is no longer receiving updates, it may be vulnerable to attack, so consider replacing it.



Keep Router Credentials Secret

Letting everybody know how to access your Wi-Fi may allow malicious actors entry into your private network. This can expose you to all the risks of a public network and more.

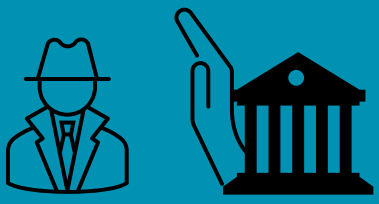
Useful Resources

- For more information on passwords, see the TechSafe good password policies booklet.
- To find your router's default password, search your router's manufacturer on: www.routerpasswords.com
- Check your router's manual for instructions on how to check its settings.

TechSafe
Business Cyber Security

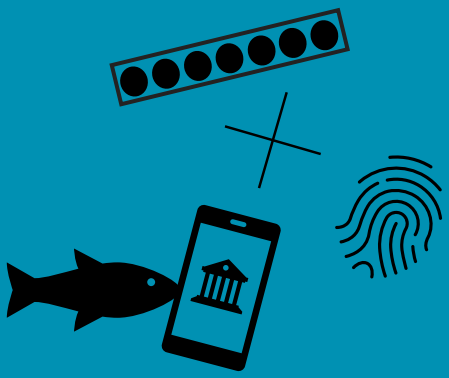
Be a Smart Phish

Secure Online Banking Booklet by TechSafe



In Confidence

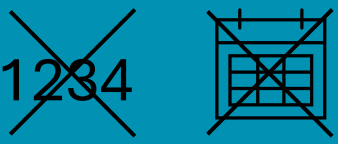
Keeping Your Account Safe



Use Multi Factor Authentication

The simplest way to improve the security of your bank account is to enable MFA.

This will make it harder for attackers to access your accounts and help you stop and think during a scam.





Choose Strong Pins

Avoid common pins, such as 1234, as well as pins with some obvious significance, such as birthdays or years. These are easy for an attacker to guess, leaving your account exposed to danger.

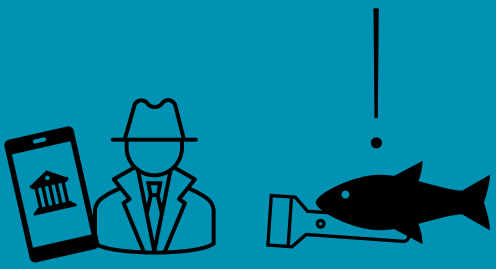
In Confidence

TechSafe
Business Cyber Security



Be Mindful of Phishing

Bank accounts are high value targets for scammers, so it's not uncommon for them to try and gain access by pretending to be from your bank. Always remember what banks will and won't ask you.



Check Your Account Often

Make sure to check you account balance and transaction history for anything strange every so often. Noticing suspicious activity early can be a big difference maker in stopping theft.

Accessing Your Bank's Website

www.bnak.co.bad

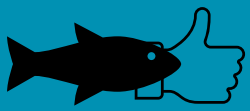


Check the URL

Fraudulent bank websites often won't have the correct URL. If you notice that the site you're on has the wrong address, even if only a slight misspelling, or a non-NZ final part where you'd expect to be connecting to a New Zealand website, leave immediately.



www.bank.co.nz

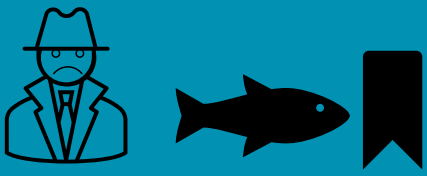


Make Sure The Website is Trusted

If when you access your bank's website your browser tells you that it doesn't trust it, close the website immediately. Even with a correct URL and layout, the website could steal your info.

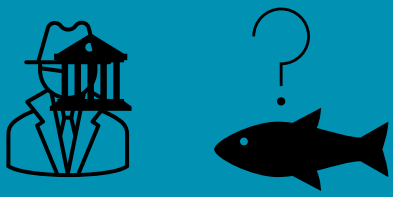
In Confidence

TechSafe
Business Cyber Security



Navigate with Bookmarks, not Links

If you need to access your bank because of an email, don't use any link supplied by said email. Instead, use the search bar, or a bookmark you know goes to the correct site.



Be Aware

Modern scammers can perfectly recreate a bank's website. Just because it looks like the real thing doesn't mean it can be trusted.

Useful Resources

- For more information on phishing, see TechSafe's phishing awareness booklet.
- For more information on multi-factor authentication, see TechSafe's password booklet.
- For information on what to do if a scammer manages to get money from your bank account, see TechSafe's phishing response booklet.

Contact information of some popular banks:

ANZ:
Phone: 0800 269 296
Website: anz.co.nz

ASB:
Phone: 0800 272 372
Website: asb.co.nz

BNZ:
Phone: 0800 735 901
Website: bnz.co.nz

Westpac:
Phone: 0800 400 600
Website: westpac.co.nz

Kiwibank:
Phone: 0800 113 355
Website: kiwibank.co.nz

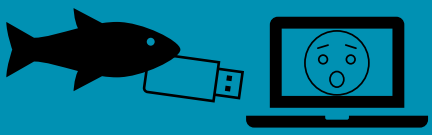
TechSafe
Business Cyber Security

Be a Smart Phish

Device and Web Safety Booklet by TechSafe

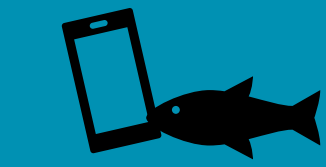
('The web' refers to the internet, where you access websites, email, social media, etc.)

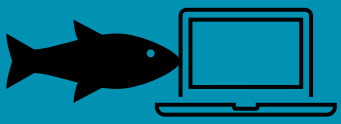
(Devices are anything that interfaces with the internet or another device)



In Confidence

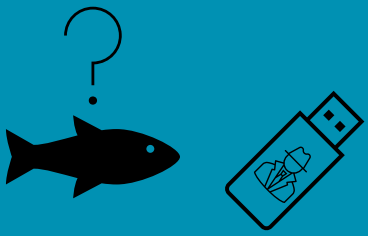
Keeping Devices Safe





Stay With Your Device in Public

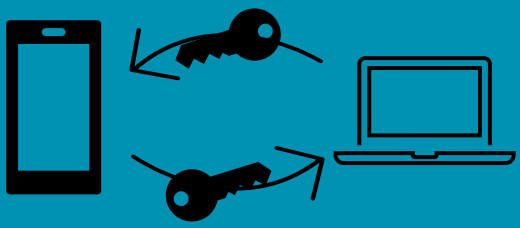
Leaving your device unattended in public, even while locked or powered off, is a bad idea. Not only could it be stolen, but attackers are able to inject malicious programs into it using devices like a USB.



Don't Trust Devices You Find in Public

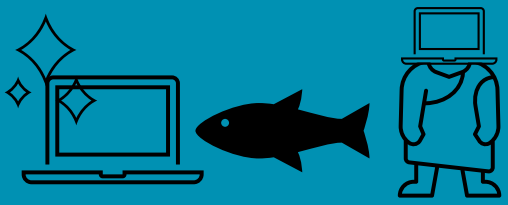
Attackers sometimes leave USBs or other devices with malicious software on them in public in the hopes someone will plug them into their device.

TechSafe
Business Cyber Security



Keep Your Multi-Factor Authentication Device Separate

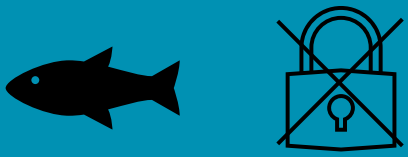
You should use a method of multi-factor authentication which is on a device other than the one you use to access the account. This helps secure your accounts, especially in the case of device theft.



Replace Obsolete Devices

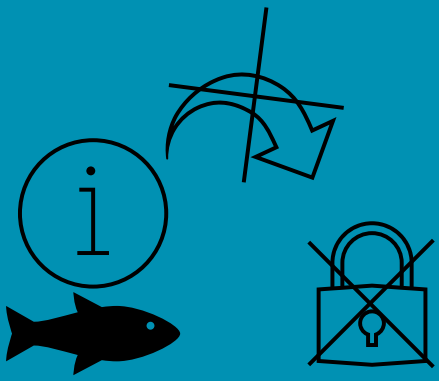
Devices are only supported with security updates for so long, and when they stop receiving them, they may become vulnerable to modern attacks. Your device will likely tell you when it's out of date, so consider replacing it when that happens.

Staying Safe on the Web



Watch Out for Insecure Sites

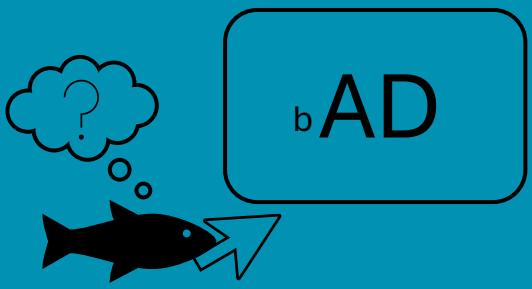
Some websites won't be trusted by your browser. Untrusted websites haven't properly verified who they are, and so could be a fake an attacker has sent you instead. Leave any untrusted website as soon as possible.



Keep Data Out of Insecure Websites

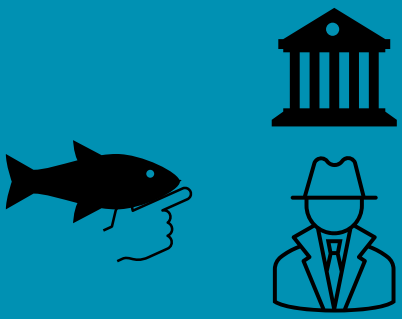
If you really need to access an insecure website for whatever reason, make sure not to enter any sensitive data. Anything you enter may fall right into an attacker's hands.

TechSafe
Business Cyber Security



Think Before You Click

Malicious actors often pay for fake ads meant to imitate legitimate website functions, such as downloads. These redirect to websites they control and, in some cases, just entering these can be dangerous. When something appears out of place, check if it's an ad before clicking it.



Be Aware of Normal Practice

Knowing what a website normally will and won't do will help in recognizing fake and malicious websites. For example, a website will never ask you to run a command to verify your identity.

Useful Resources

- For more information on recognizing forms of phishing other than fake websites and ads, see TechSafe's Phishing Awareness Booklet