Spotting:

Scams & Malicious Acts

Created Date: 10/07/2013
Update Date: 01/07/2026

Ver. 13.0

Scams have become more rampant over the years.
They cost organizations around the globe averagely $4.5 billion every year and over half of internet users get at least one phishing email per day.
In **2025**, reports from organizations such as **Scamwatch**, **ReportCyber**, and other entities were combined, showing that Australians reported losses of **$2.18 billion**, which has increased from last year, which is unfortunate. While scammers continue to become more sophisticated and adapt their methods, including the use of emerging technologies such as Artificial Intelligence (AI), reported losses remain well below the peak experienced in 2022. This is due in part to the continued efforts of Law Enforcement, Government Agencies, Organizations, Information Communication Technology Organizations, White Hat Hackers and Scam Baiters. Initiatives by these groups help people become more aware, remain vigilant, and better protect themselves against scams.

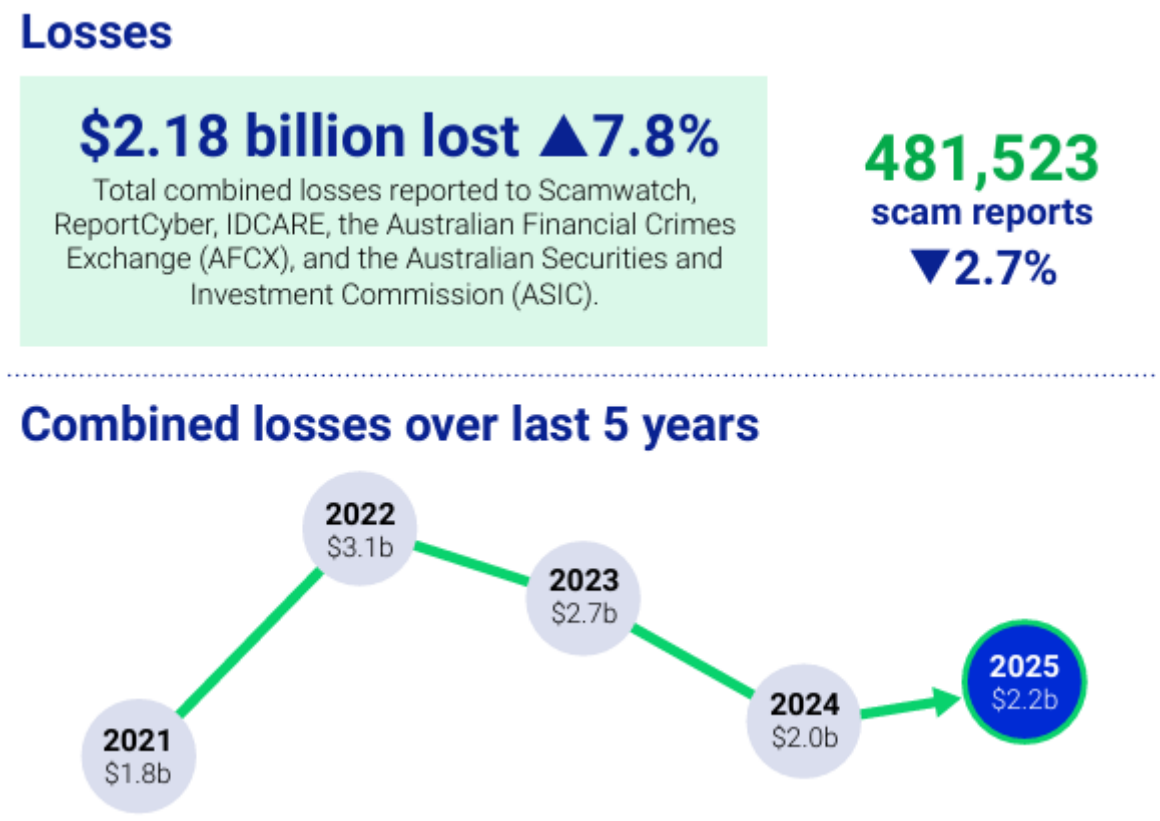


Figure 1: Supplied by SCAMWATCH

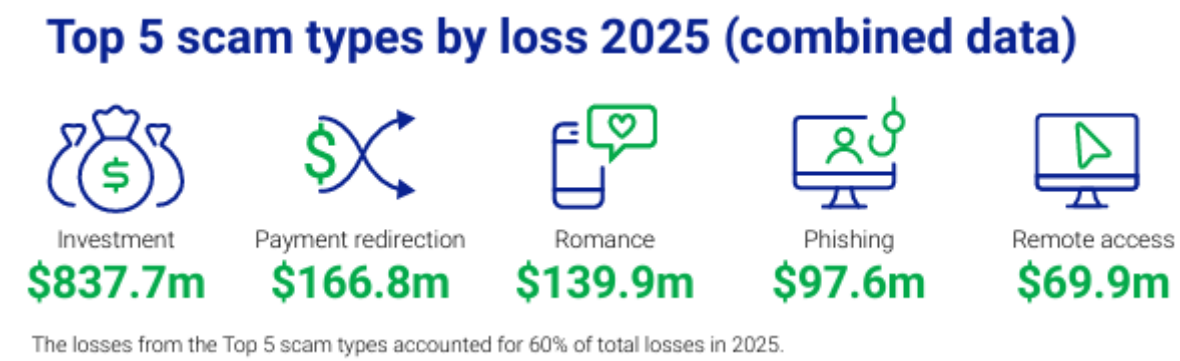


Figure 2: Supplied by SCAMWATCH

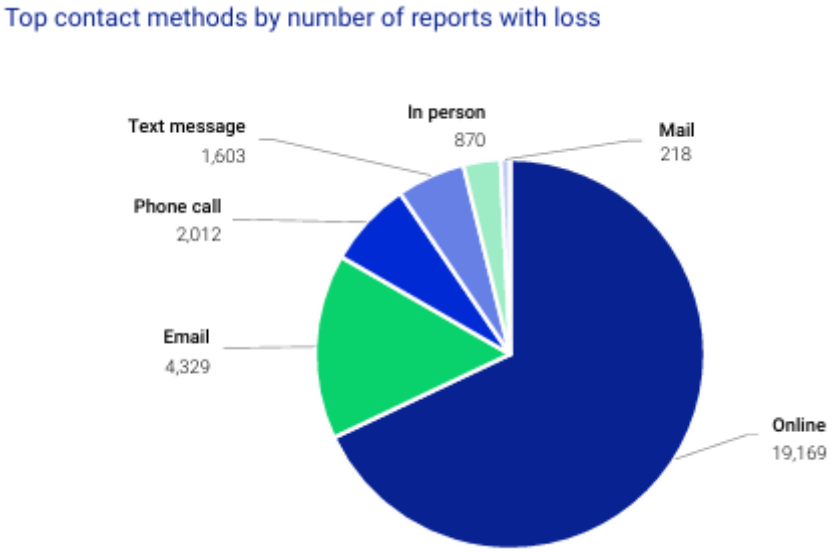


Figure 3: Supplied by SCAMWATCH

Investment Scams continue to result in the highest financial losses reported in Australia, with Cryptocurrency and fraudulent investment opportunities remaining common methods used by scammers. However, Australians continue to be targeted through many different channels, including phone calls, emails, text messages, social media, messaging applications, online marketplaces and compromised or fake websites.

Artificial Intelligence (AI) is now being widely used by threat actors to create more convincing scams. AI can generate realistic emails, fake websites, cloned voices and even deepfake videos that make it increasingly difficult to distinguish legitimate communications from fraudulent ones.
Scammers constantly adapt their techniques to take advantage of current events, new technologies and human emotion. Remaining vigilant, verifying unexpected requests and taking a moment to Stop, Check and Protect yourself before acting are some of the most effective ways to avoid becoming a victim.

The following information explains some of the most common scams affecting Australians today, along with practical advice to help you identify malicious attempts and protect yourself, your family and your business.

What Scams can you come across?

There are many different scams that have been created over the years, many of which are constantly adapted to target specific countries, individuals, and current world events.
Here is a list of common scams actively used across Australia:

Romance Scams

These scams involve fraudsters who target individuals looking for a significant other online, carefully building up a relationship over time, often posing as someone living in another country.

The scammer invests significant time and effort to elevate the emotional connection to a high enough level where the victim becomes willing to help with nearly any request.
Once trust is established, the scammer will typically request "Emergency Funds" to assist a sick or dying relative, a distressed pet, or themselves. Alternatively, they may request funds to cover travel expenses or visas to come to Australia to meet in person.

They almost always insist on having money sent to an overseas bank account, often registered under a completely different persons name or in a third-country jurisdiction - sometimes both.

Remote Access Scams

In these types of scams, the criminal will most commonly make direct contact via an unsolicited phone call. Other entry points include website breaches, fake/cloned websites, or malicious pop-ups indicating that your computer has malware or viruses.

These scammers typically pretend to be from a well-known technical infrastructure or support company.
Internet-driven variants utilize malicious browser pop-ups or system alerts claiming your device is heavily compromised and ordering you to call a specific number displayed on the screen for immediate help.

Phone-driven variants frequently impersonate:

- Tech Support giants like Microsoft, Apple, or Google
- Internet Security/Antivirus companies like McAfee, Norton, or Malwarebytes
- Major Telecommunications providers like Telstra, iiNet, or Aussie Broadband

The scammer will aggressively request remote support access to your device (commonly a Windows or Mac computer) so they can supposedly “fix your problem”.

They will invent convincing scenarios, such as claiming your device has been hacked, that it is broadcasting malicious traffic across the web, or that there is a critical fault with your NBN/internet connection, all to coerce you into initiating a remote connection session.
Scammers intentionally leverage completely legitimate commercial software that they instruct you to download and install, such as TeamViewer, AnyDesk, or LogMeIn.
Once inside, they routinely open the Windows “Event Viewer” App that is built-in to show you ordinary, harmless background operational warnings, falsely claiming these represent severe hacker activity or destructive viruses. Alternatively, they open the Command Prompt (the black text screen) and execute “basic commands” to run what looks like a system scan.
While the text scrolls past, they will manually type an “error” or “infected” message directly into the terminal window to terrify you.

They will then pretend to “clean” your computer of these non-existent threats and will often attempt to install third-party software under the guise of providing ongoing security and protection.

Crucial Fact: Nobody knows there are issues with your machine except **YOU**. If you have not actively sought out technical support yourself, any incoming warning or offer to fix it is a scam!

If you notice strange background activity or unclosable pop-ups directing you to contact a support line, immediately turn off your computer and seek trusted local technical support, such as CPKN Computers.

If you receive an unexpected phone call regarding technical issues with your computer or internet connection and the operator demands remote access, collect as much identifying information about the caller as possible while volunteering zero details about yourself.

Document their stated name, the “company” they claim to represent, the incoming phone number, and any other specific details they offer.

Firmly state that you will handle the matter directly with your local IT support company. If they attempt to pressure you or argue against it, simply tell them you are keeping the computer turned off and hanging up. Disengage immediately if they do not comply.

Refund / Money Mule / Lottery / Inheritance Scams

Scammers utilize sophisticated social engineering frameworks designed to extract direct payments or access your accounts under the false pretense of sending funds to you.

Refund Scams: These are heavily prevalent and frequently involve automated or live calls claiming to be from Amazon or major retailers. They inform you that an error occurred or that “suspicious activity” was detected on your account, which they claim they are happy to cancel and fully refund to you.
When you agree to process the refund, they will almost always employ the “Fake Transfer” technique, which strictly relies on gaining remote access to your computer. Any refund process that requires remote access to your personal device is **ABSOLUTELY** a scam.

Legitimately, a corporation already possesses the tools to reverse a transaction directly to your payment card or will ask cleanly for standard bank routing/transfer details to deposit it. If an entity demands card credentials to issue a refund, tell them to use bank transfer details only.

Once they gain remote access to your device, they instruct you to log directly into your online banking portal - this is where the manipulation occurs.

They will direct you to your account transaction history screen, and then deliberately black out your monitor using remote software tools under the guise of “processing the transaction securement”. While your screen is dark, they use the web browsers built-in developer tools to modify the code displayed on your screen, altering your visible balances to make it appear as though a massive overpayment has landed.

They utilize various scripts to execute this, but once complete, they restore your screen and initiate a panicked “cry baby” script.

For example, if your expected refund was $250, they will show an account balance that has had several zeros appended, displaying $25,000. The scammer will fake absolute panic, begging and pleading for your help to return the “accidental overpayment” to save their job.
They calculate the numbers based on what your account can afford to move.

They will then direct you to wire the excess funds to an external account or instruct you to purchase retail gift cards to cover the difference minus your original refund.

Money Mule Scams: These can operate as one-off transactions or ongoing arrangements.

You may encounter a realistic job advertisement seeking an “Account Manager” or “Transfer Agent”.

These roles offer high work-from-home pay with very basic entry requirements. Your role is simply to receive funds into your personal bank account and then transfer them onwards to an external account.

Because your personal account looks established and legitimate to bank fraud departments, scammers use you as a clean conduit to launder stolen money.

One-off variants promise a large payout you will never receive; ongoing roles offer commissions based on the total volume handled.

Lottery, Investment & Inheritance Scams: These communications claim you have been awarded
or left a massive sum of money for a specific reason, or request your urgent assistance in handling or moving wealth. Before any funds can be released, you will be ordered to pay upfront “transfer fees,” “taxes” or “legal clearances” directly to the scammer.

Once you pay these upfront fees, the communication cuts off, and the promised fortune never materializes.

Tax / Arrest Warrant Scams

This widely distributed scam relies on intimidating phone calls, automated robocalls, or official-looking emails stating that you owe an outstanding tax debt, or that an official Arrest Warrant has been issued in your name due to tax fraud or illegal activity.

You will be offered an immediate opportunity to settle the debt or pay legal fees to cancel the warrant. They will demand payment via unusual, untraceable methods, including retail **GIFT CARDS** (**An Immediate Red Flag!**), crypto assets, or rapid wire transfers.

Note: Countless alternative scams - such as fraudulent solar installation rebates, car insurance schemes, and aggressive door-to-door sales operations - are actively operating across Australia. It makes knowing who to trust increasingly difficult.

What Can Be Done to Tackle Scams and What Are Signs It's Fake?

The primary pathways scammers use to target individual citizens are direct phone calls, SMS text messages, and phishing emails.

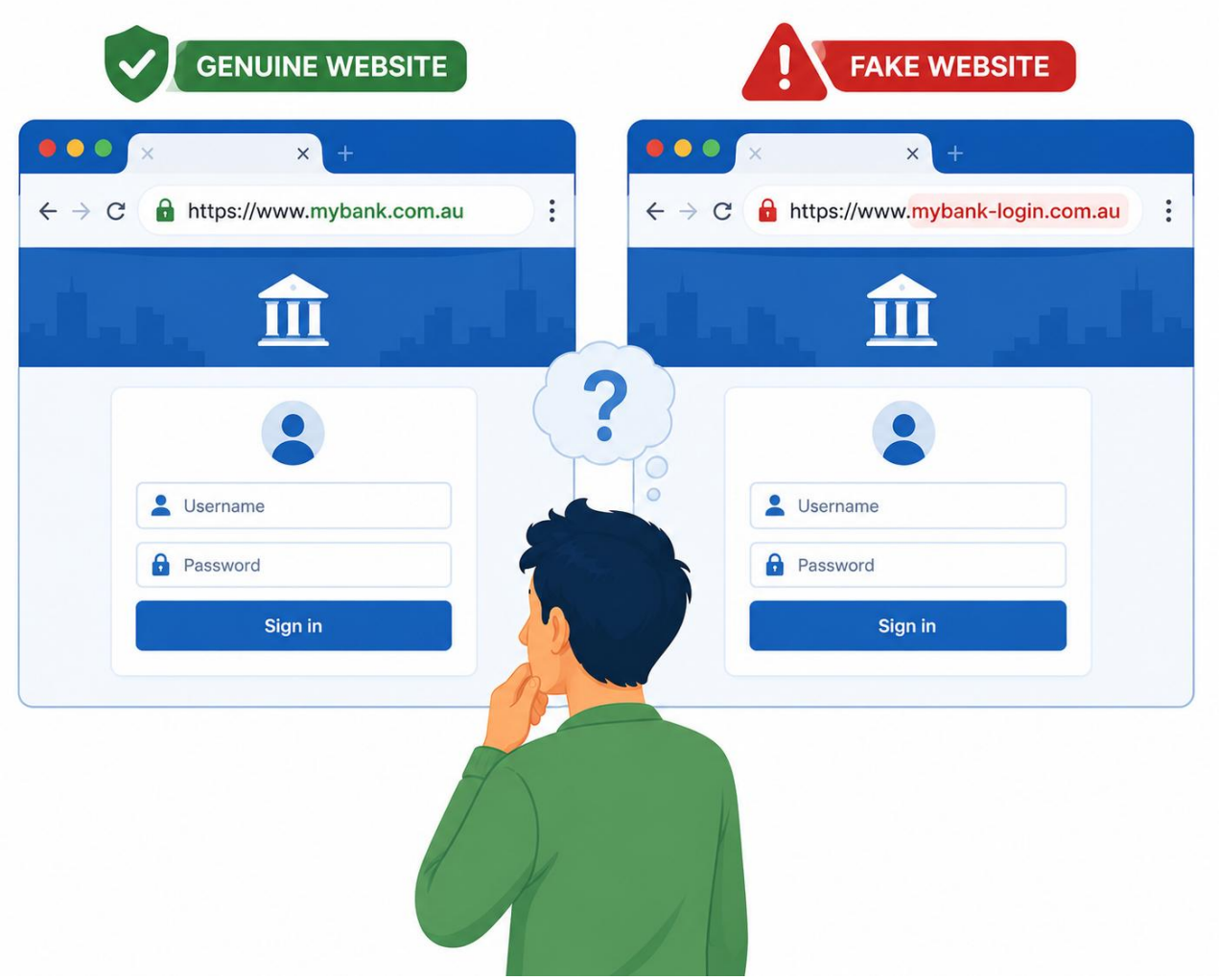
Calls can stem from any scam configuration, ranging from fake Amazon refund lines to aggressive tax fraud arrest threats. SMS text messages leverage identical refund scripts, but in recent months, fraudulent package delivery links have heavily targeted Australian mobile numbers.

Emails reflect these same tactics. Most commonly, you will receive fraudulent billing notices or fake banking alerts claiming you owe an overdue balance or have an outstanding credit waiting.

Phishing emails are designed to capture your exact login credentials for high-value platforms like Facebook, PayPal, eBay, Amazon, and major banking applications.

The broader web also presents structural risks. You may click an article link that directs you to an external website requiring you to fill out a form or download an application. This is a common trap. For example, a compromised Facebook account belonging to a trusted friend might post or message you a link to an interesting news article. When clicked, a fake login page prompts you to enter your Facebook credentials to view the content. Because it originated from a trusted friend, victims log in - only to realize the article did not require a login, and they have just handed their account access directly to cybercriminals.

Websites can be either completely compromised or systematically spoofed (cloned). Compromised legitimate websites are used to trigger unauthorized malicious pop-ups, such as the fake Microsoft technical alert ordering you to call a specified helpline. Spoofed websites are perfect visual clones of everyday services, engineered specifically to harvest your banking or corporate credentials.

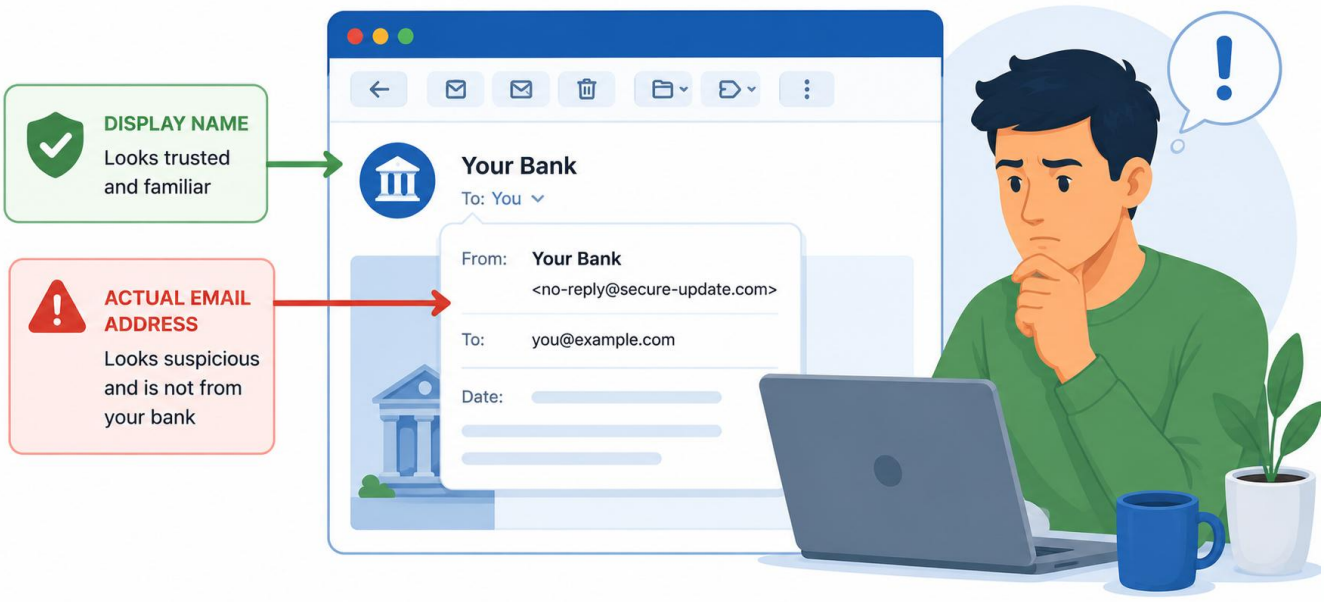


Critical Signs & Solutions:

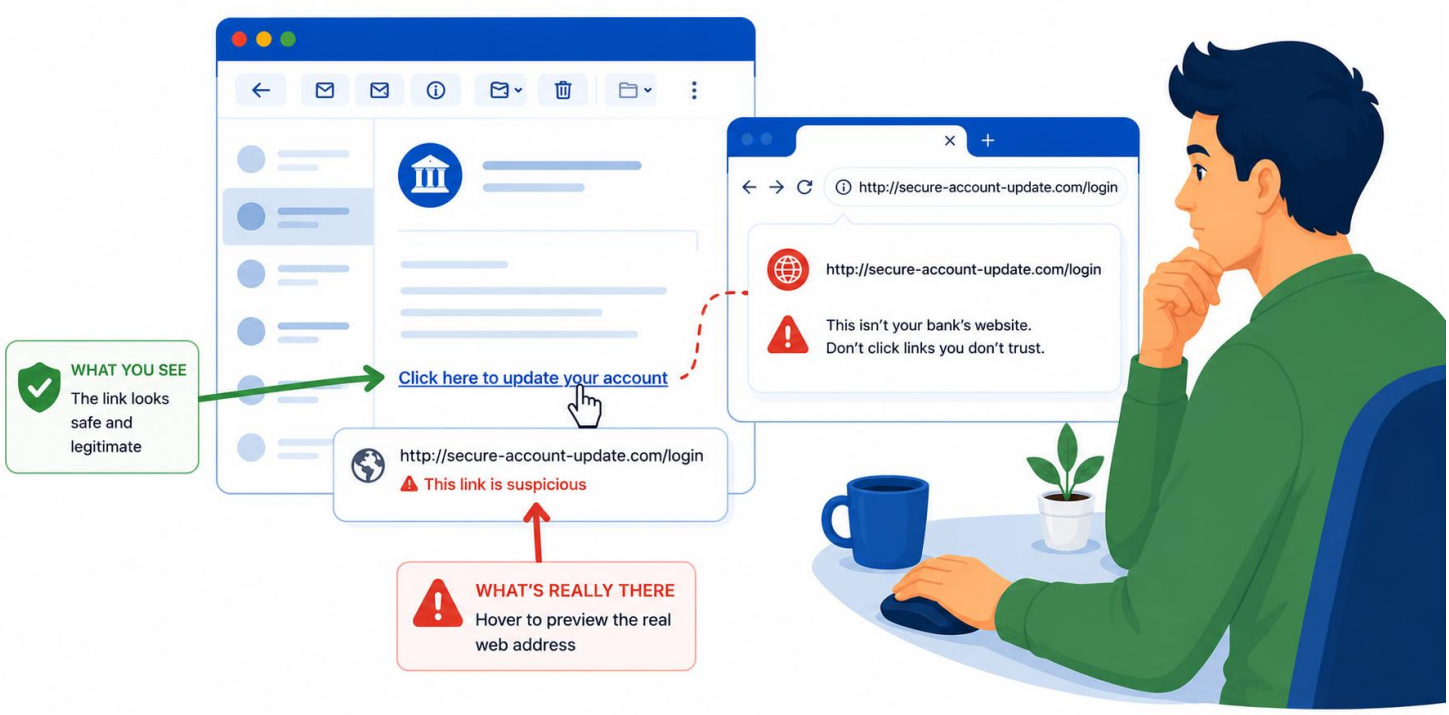
For emails, the strongest foundational defense email providers possess is blocking malicious messages before they ever hit your inbox using the DMARC (Domain-based Message Authentication Reporting and Conformance) standard. DMARC applies a digital ownership verification tag to a specific domain (such as “@cpkncomputers.com.au”). Because our domain is strictly mapped to our legitimate business servers, any incoming message claiming to be from us that lacks this verified digital approval tag will be automatically rejected or flagged.

Unfortunately, some sophisticated phishing emails will always slip through the cracks - research indicates that up to 97% of people globally cannot accurately identify a highly sophisticated phishing email.

- **Don’t Trust the Display Name:** A premier tactic among cybercriminals is spoofing the visible display name of an email. Security data analyzing over 760,000 email threats targeting major global brands revealed that nearly half explicitly spoofed the brand name in the display field. For example, a scammer can format an email to display as “My Bank<accounts@usbank.ru>”.
  Because the actual underlying domain is “usbank.ru” and not the legitimate financial domain, a standard DMARC policy on the real bank’s domain won’t block it automatically. The email lands safely in the inbox because mail applications prominently display the friendly name, leading users to believe it is authentic. Always inspect the exact, underlying email address.

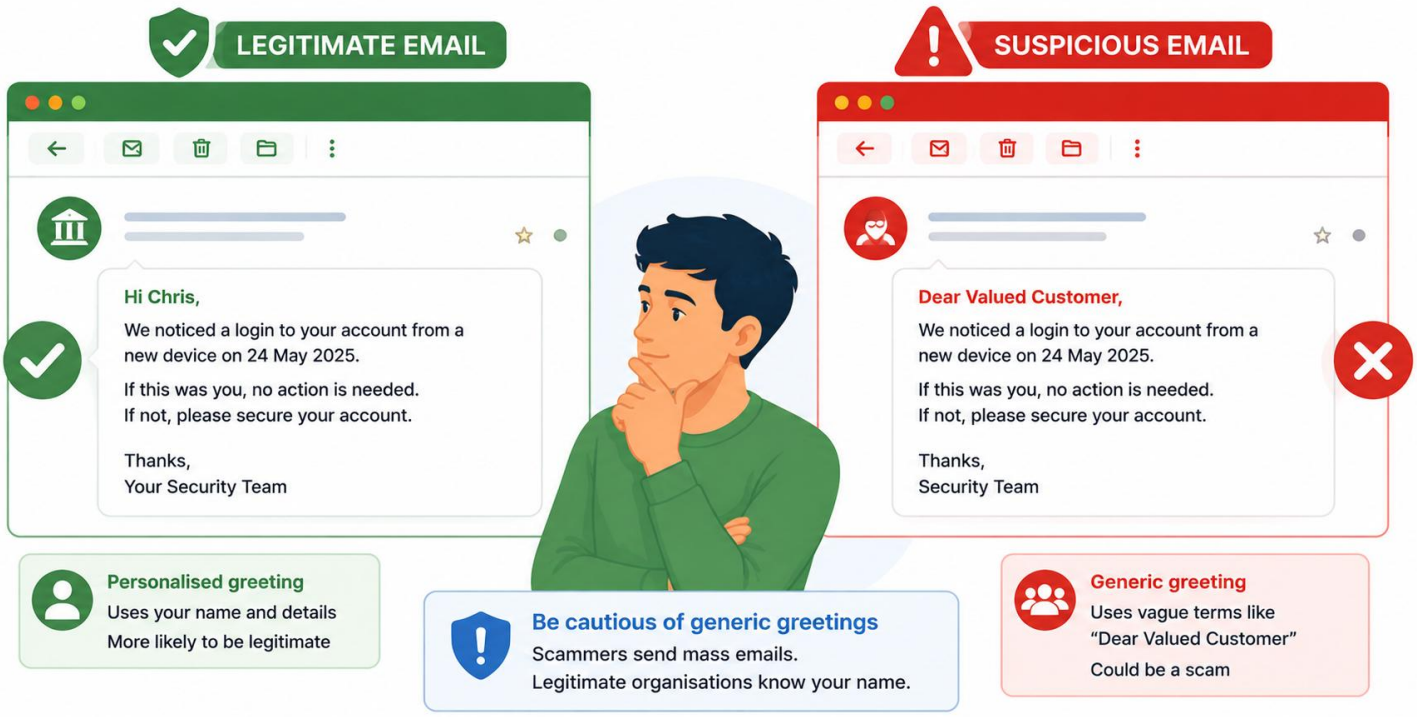


- **Look But Don't Click:** Hover your mouse cursor over any embedded link within an email body without clicking it. A small text bubble or pop-up should appear near your cursor or at the bottom of your browser/mail application window, showing the true destination URL. If the web address looks unusual, irregular, or completely unrelated to the sender, do not click it. If you cannot safely preview the link destination, leave it alone. Mobile devices and tablets do not handle link previews as cleanly; for these devices, it is safest to copy the link text directly and paste it into a verified link checker. To safely evaluate suspicious URLs, visit our website to use our link checkers: cpkncomputers.com.au/scam-support



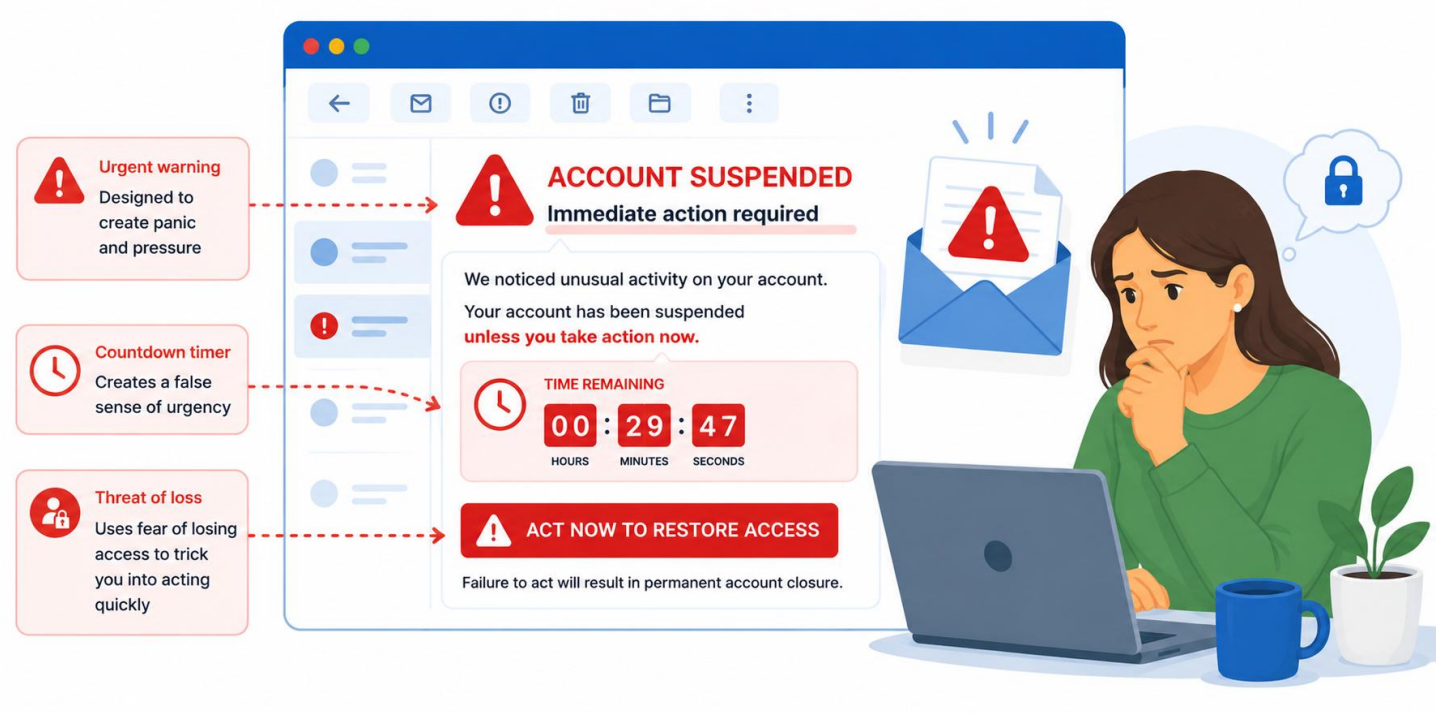
- **Check for Spelling and Grammar:** Established corporate brands maintain strict standards for communications. Legitimate corporate text messages or emails rarely contain glaring spelling mistakes, broken phrasing, or poor grammar. Read your communications precisely and treat linguistic errors as immediate red flags.

- **Analyze the Salutation:** Is the communication addressed to a generic title like “Valued Customer” or “Dear Account Holder”? Legitimate businesses with which you hold an account will almost always address you directly by your registered first and last name. Treat generic salutations with extreme skepticism.



- **Don’t Give Up Personal Information:** Legitimate financial institutions and major corporations will never request your passwords, PINs, or secondary security codes over email or SMS. If you receive an urgent message demanding that you “verify” your identity or unlock an account via a link, do not reply or click. Instead, contact the organization directly using a known, verified phone number from their official website to confirm.

- **Beware of Urgent or Threatening Language:** Instilling a sense of immediate urgency or fear is a core psychological tactic. Be highly wary of subject lines or notices declaring “Account Suspended,” “Unauthorized Login Detected,” or “Legal Action Pending.” Independently verify these claims by navigating to the official provider site directly through your browser.



- **Unrealistic or Extreme Threats:** Criminals use intimidation to bypass logical thinking. In Australia, scammers frequently masquerade as the Australian Taxation Office (ATO), threatening immediate police arrest or severe legal prosecution unless an immediate payment is processed. A secondary localized variant involves callers claiming to represent an “Accident Investigation Department” or a third-party complainant’s insurance firm, attempting to coerce you into settling fictitious auto accidents or policy claims.

- **Review the Email Signature:** A complete absence of structured corporate details, physical address information, or official contact pathways strongly points to a phishing attempt. Legitimate businesses provide comprehensive contact info.

- **Don’t Click Unsolicited Attachments:** Malicious attachments containing embedded malware, ransomware, or spyware remain a dominant threat vector. This malicious software can corrupt local files, harvest stored passwords, or silently monitor your keystrokes. Never open unexpected attachments.

- **Don’t Believe Everything You See:** Modern cybercriminals copy branding assets perfectly. The presence of authentic high-resolution logos, matching corporate colors, and realistic legal footers does not guarantee authenticity. Maintain a highly skeptical mindset.

- **Offers That Seem Too Good to Be True:** The classic rule remains absolute: if an offer looks impossibly lucrative or beneficial, it is almost certainly a scam. This is especially true for random SMS messages or blind emails promising unexpected financial windfalls.

- **Unsolicited Contact Regarding Technical Faults:** If you receive an out-of-the-blue phone call from someone claiming your phone, laptop, or NBN connection is experiencing technical errors, hang up. Telstra-themed scams often involve operators claiming your “IP Address has been hacked” and that your local device protection is insufficient, requiring them to “install IP security adjustments”. This is logically flawed: if a real technical fault existed on their network infrastructure, the provider would resolve it at the infrastructure level without requiring access to your local machine or demanding private compensation.

- **Demands for Unusual Payment Methods:** Scammers consistently demand payment via non-reversible, untraceable methods. If any entity requests payment via pre-loaded debit cards, retail gift cards (such as iTunes, Google Play, or Amazon), cryptocurrency, or rapid international wire transfers, it is a scam.

- **Demands for Remote Access:** Remote access software is a highly legitimate tool utilized daily by trusted technical professionals to solve complex issues efficiently.
  For example, CPKN Computers securely utilizes verified, encrypted remote access systems to assist clients. However, if an incoming caller or unsolicited pop-up instructs you to grant them remote access to your system out of the blue, deny it entirely. Never grant access unless you initiated the support request directly with a known, trusted local firm.

- **High-Pressure Tactics:** Scammers create intense psychological pressure to force rapid compliance before you can consult a family member or an IT professional. They will threaten immediate account termination, legal action, or system damage if you hesitate. Slow down and take control.

Handling Phone Calls

When receiving an incoming call from an unrecognized number—especially mobile configurations or private caller IDs - it is critical to maintain strict vigilance regarding the caller's true intent.

An Immediate Red Flag: A representative claiming to speak on behalf of a large corporate entity or a federal government department calling directly from a standard mobile phone number.

If the caller addresses you by name, do not explicitly confirm your identity. Instead, calmly use a neutral screening phrase: "May I ask who is speaking and the specific nature of this call, please?"
Force them to identify themselves and state their clear business objective first.

If anything feels wrong or triggers an uneasy intuition, keep your spoken words to an absolute minimum and actively disengage from the call.

Ask structured questions: Demand their full name, their employee identification, the exact company they represent, their official callback number, and a formal reference number for the matter. Document their accent, demeanor, and responses clearly. Do not volunteer or validate any personal information.

If you feel uncomfortable, explicitly state: “I will review this matter independently and contact your organization back through official channels”.
Locate the verified, publicly listed contact number of the specific business or government agency directly from their official website or an official directory. Call them back to verify if the contact was legitimate. If you remain completely unsure, disconnect the call immediately and seek guidance from a local IT professional or visit a local corporate branch in person.

Strategic Security Recommendations

To comprehensively safeguard your personal and/or business infrastructure, we recommend implementing the following:

- While built-in tools like Microsoft Defender and Apple Security offer excellent baseline protection against everyday, known threats, modern cybercriminals use sophisticated techniques - like fileless malware and remote access scams - that can bypass standard antivirus.
  To ensure complete protection, we recommend upgrading to an advanced endpoint security system that actively monitors system *behavior* and blocks malicious activity in real-time.
  For Home & Business Users, we provide premium endpoint protection (EDR) that goes beyond basic scanning, offering advanced defense against identity theft, deceptive scams, and ransomware protection with automated rollback capabilities to keep your personal data safe.
  Businesses can also benefit from other security frameworks and proactive monitoring through our comprehensive Managed Services. For details, request information on our **Business Management Service (BMS)**.

- **Utilize Spam and Scam Mitigation Apps:** Deploy verified call-filtering applications, such as Truecaller, on your Android or iOS devices. These utilities provide crowdsourced spam identification, real-time caller tracking, and automated blocking of known fraudulent numbers.

- **Verification Principle:** If a person contacts you via email, phone, SMS, or post claiming to represent an official organization and you harbor any doubt, do not utilize any contact links, phone numbers, or credentials provided within that communication. Always navigate independently to their official, public web domain to secure their legitimate contact information.

If you are uncertain about a communication, contact CPKN Computers directly for expert assistance. We provide a complimentary Free Scam Check to help you verify suspicious messages.
Always report active scam operations directly to us or lodge a formal report with Scam Watch - An Australian Government Division.

Please refer to the Created Date and Revision Number on the Front of this Document.
If you think you do not have an Up-to-Date Version, please ask for one from CPKN Computers.

ABN: 72 930 048 407
Phone: 02 6138 5012
Web: www.cpkncomputers.com.au
Email: support@cpkncomputers.com.au