# Cyber Safety Guide

GR LEGAL
LAWYERS AND BUSINESS CONSULTANTS

In our commitment to your digital safety, we would like to shed light on some essential cyber security practices, especially in relation to interactions with our firm.

In today's digital landscape, it's important to remain vigilant as cyber threats continue to evolve. At **GR Legal**, we do everything in our power to keep you safe, but it is still imperative to be cyber aware.

Cybercriminals might approach you through emails, SMS, or phone calls with the aim of deceiving you. Be vigilant and stay mindful of these simple yet effective tactics.

## Our promise to you

We will never ask you to confirm your personal details or account information through email or SMS. We will use more secure methods, such as a secure website or via a direct phone call to the number you supply us with.

If you receive a suspicious email or SMS request, it's crucial to verify the authenticity of the requestor before sharing any personal information. You can do this by contacting us directly through our official website or phone number, not through the contact information provided in the suspicious message.

If you have concerns about potential fraud in relation to your matter, please report this to us immediately through **www.grlegal.com.au or via telephone on (03) 9755 8345.**

## Our top cyber safety tips

**Do not click on suspicious links** or download unknown attachments, even if the sender looks like a trusted source.

**Secure your devices** by password protecting your phones, tablets, laptops, and computers and installing an antivirus software. Ensure you are keeping your devices up to date, as providers often release security enhancements.


**Choose secure passwords or passphrases** that use four or more random, unrelated words as your password. The longer, more unpredictable, and more unique, the stronger the password will be.

**Secure your accounts** by using multifactor authentication (MFA). MFA is a security measure that requires two or more proofs of identity to grant you access.

## Where to report a cybercrime

Australian Federal Police recommendations

If you encounter any form of cybercrime or have concerns about potential fraud, remember that you have options:

- Contact your local law enforcement agency
- Utilise resources like Scamwatch, a government initiative focused on providing guidance about scams and cyber threats.

If you received a suspicious looking email that appears to have been sent by **GR Legal**, for your safety, DON'T click on any links or attachments in the email. Please get in touch with us immediately.

## Cases of fraudulent activity

Australian homebuyers, Simon Elvins and his wife, endured a heartbreaking ordeal when they lost nearly **$250,000** to a payment redirection scam. Having saved for 10 years to purchase their first home in the Blue Mountains of New South Wales, Simon received an invoice via email from his conveyancer requesting payment for the initial home deposit. Unbeknownst to him, scammers had intercepted the email and altered the account details. Within two transfers, the couple lost **$274,311.57**. Despite their efforts to recover the funds, they received only a fraction of it back, leaving them with a more substantial mortgage than anticipated.

Read the full story here.

John and Julie, a Melbourne couple, faced a holiday nightmare when they discovered their bank accounts were being drained due to identity theft. Despite notifying their banks and credit card providers before going overseas, they lost at least **$325,000** to fraudsters who created 20 credit and debit accounts in their names.

Read the full story here.