Cyber security is central to wealth protection.

With heightened digital activity amid the pandemic, cyber security has come into sharper focus. Vigilance is required to safeguard the assets and privacy of high net worth individuals.

An average of 164 cybercrime reports are made by Australians every day.[1] That equates to one cyber-attack reported every 10 minutes, with a large percentage of the increasingly sophisticated attacks going unreported.

For individuals with greater financial resources, prominent or easily accessible online public profiles and extensive personal and professional networks, the cyber threat can be elevated. So, as the lines blur between digital and physical activity, exacerbated by more than a year of remote working for many, it is timely to examine the ever-present cyber risks and how to protect against them.

Luisa Genovese, CommBank's Executive Manager of Cyber Resilience and Recovery, says that the economic distress experienced in many countries due to the pandemic is spurring an increase in cyber crime.

"Cybercriminals like to use themes of the day, leveraging people's innate curiosity and trust to conduct scams, fraud, and identity theft, and playing on the impact of the pandemic is widespread," Luisa says. "They're not only looking for financial gain or personal details but to enhance their reputations within their criminal networks by luring in high-profile targets."

[1] Australian Cyber Security Centre, Annual Cyber Threat Report (July 2019 to July 2020).

Common cyber threats

The more invested assets you own that are easily transferable, such as cash, shares and bonds, the more appealing you may be as a target. High net worth individuals often have multiple parties managing their financial affairs, expanding the scope of potential vulnerability.

Luisa says that while the themes used to deliver a cyber attack have changed, the nature of the attacks is largely unchanged, with ransomware and email compromise the most common.

"Ransomware is a type of malicious software, or 'malware,' that once it's on your device, makes your computer or its files unusable until a ransom is paid to the cybercriminals," Luisa says.

> *"The pandemic has led to a sharp uptick in the speed at which attackers can exploit vulnerabilities in remote connections, which they can then leverage for ransomware attacks."*

Email compromise is also increasing as attackers use various methods to impersonate authority figures and spread fraudulent invoices or requests for money transfers. Spear phishing (emails designed to get targets to reveal confidential information) and highly targeted scams require individuals, and by extension their families, to be diligent with cyber hygiene.

Safeguarding your identity

Cyber criminals also work to identify targets and research their digital footprints to create a comprehensive picture of an individual's identity that can then be used to conduct fraud. They often use open-source platforms such as Facebook and LinkedIn to gather information, attempt social engineering on staff and family members and craft a custom spear phishing email, account take over or other more sophisticated attacks.

"High profile and high net worth individuals need to be aware of the real risk of identity theft or having personal details harvested and stored, potentially to be auctioned over the dark web to the highest bidder," Luisa says.

"Be selective and strategic about what information is made public and what is kept private and be aware that this extends to family members who may be inadvertently revealing information that can be used in an attack."

Key measures to adopt

Update software

Updating software and apps once an update is available is a simple yet critically important measure. In the time between the update release and it being implemented, attackers gain access, so it is best practice to set software updates to automatic.

Disciplined email and SMS correspondence

With a reliance on email communication, it is imperative to verify who you are talking to and avoid sharing valuable information. Voice or face-to-face is a safer option for many sensitive conversations. Remember, CommBank or Commonwealth Private will never ask for your banking information by email or text message.

Limit information sharing

Criminals can glean information from social media, including LinkedIn. Containing your digital footprint can make it more difficult for criminals to customise an attack.

Security controls

Many controls used in larger companies need to be employed in a home or personal setting. This includes using two-factor authentication for all accounts that hold sensitive personal or financial information. Use hard to guess passwords or passphrases that you change regularly.

Be wary of apps

Be careful which apps are installed on your phone and the permission settings within those apps, which can provide access to your contact lists, files and location. Only use apps from an official app store and do not click on unsolicited links received via emails or text.

The Commonwealth Bank partnered with the Australian Government's Australian Cyber Security Centre to help protect clients against cybercrime.

Find out more at **commbank.com.au/support/security**

Before you go...

If you're ever unsure whether an email sent to you by CommBank or by your Commonwealth Private Banker or Private Wealth Manager is legitimate, please don't hesitate to call us straight away.

commbank.com.au/**commonwealthprivate**