REESBY.

50+ CYBERSECURITY TIPS

www.reesby.com.au

REESBY RECRUITMENT

SPECIALIST TALENT

ABOUT US

Reesby are a specialist IT Recruitment Agency. Reesby have launched technology events across Victoria, we were a key organiser of the Victorian Engineering and IT Expo that had 3,000 graduate attendees and exhibitors which we brought together such as Commonwealth Bank, Thales, Dolby Digital, Telstra and so much more! We have been nominated in 2016 for the TechDiversity award and we have a division that specialises in Women in IT. We also have an IoT Division with access to emerging tech talent

SERVICES & OFFERINGS

We provide an outgoing high quality of client service to ensure convenience and seamlessness with a fresh approach to recruitment. We assist with staff on boarding, staff retention strategies and also attracting talent to your organisation who may not have considered a role with your business previously. We provide police-checks through Intercheck, who are the provider of background checks for Deliveroo. It is important you get quality and verified talent!

SPECIALIST RESOURCES

- Web, Mobile, Software, Hardware, Robotics Engineers
- Firmware, Wearables, Embedded, Electronics Engineers
- Automation, Network and System Engineers
- Digital, Social Media, Marketing, UX/UI, Graphics Talent
- IoT, AI Experts, VR/AR Experts, M2M Experts
- Program Managers, Project Managers, Program Directors
- C-Level and Executive Senior IT Management CIO/CTO
- Female Candidates Across all IT Sectors for Equality
- Testers, IT Support, System Admin and Technical Support
- **Cyber Security Experts and Penetration Testers**

TIPS

- "Call an expert to check the settings on your kids' devices. Ours are quite safe, but the kids have very few protections" -Tracey Spicer TV Presenter / Columnist Fairfax Media
- Do not disclose your full address or passport information on your resume
- On mobile apps always select location services "only while using app"
- Always turn off geolocation settings when they aren't needed on a device
- Do not enter your credit card details on sites which say "check if your credit card is stolen"
- Use a password generator and have difficult passwords everywhere and keep changing it
- Use encryption or encrypted services with confidential documents
- Be aware and careful with your digital footprint
- Do not add people you are unsure of on social media
- Report or block users on social media if you feel its spam or fake
- Have restricted access to your online profiles so that only people who know can reach you. Do not share it to public
- Do not leave devices in unattended vehicles, even when locked
- Have the latest antivirus and firewalls to keep your content secure
- Always keep your software up to date, even on your smart TV
- If you receive an email that looks a little off, check the sender's email details to confirm if the address matches the organisation it is supposed to be coming from
- Use a password or identity management solution
- Treat your password as your toothbrush, change it often and don't share it
- Always check the website domain name before logging in to a website
- Do not use the same credentials while registering to other websites using your email IDs
- Avoid using banking credentials on HTTP websites, it is ideally HTTPS
- Try avoiding "Remember passwords" in the browser
- Try avoiding using "remember form fill in details" particular for credit card details
- Be cautious while installing free software on your system. Check if the source is legitimate
- For mobile applications check for the permissions apps request while installing applications for playstore/appstore
- Make sure to update your windows system and database of antivirus frequently
- Be wary of your online discussions, if you cannot see someone or hear their voice it may not be the person you think it is.
- Be wary of using free public wifi, avoid wherever possible
- Do not connect USB sticks to the network or allow the uncontrolled use of USB sticks. It is still an easy way hackers access systems or people steal data.
- Don't leave unattended servers on system check them regularly
- Don't leave a reception desk computer unattended
- Always have a time-stamped sign-in system or strategy for visitors to your office or building
- Be mindful of the data on any iPad used to check-in office visitors
- Check your computer safety before you access critical devices
- Employ a full-time cybersecurity specialist
- Do background checks on employees

CONTINUED

- Never use your real date of birth on any online service (especially social ones!)
- If you are selling something online don't pay anything to the person buying to be able to sell, only pay ad post fees to the website.
- Be mindful of applications you make online such as jobs, credit checks or loan calculators and ensure the website is legitimate
- Do not leave your devices unattended...EVER
- For executives or senior management, ensure you have a disposable clean device provided for travel. Quarantine them upon return from overseas trips
- Train your staff and test them to ensure they are safe online
- Be cautious using free hotel wifi overseas
- Purchase an anti-skimming wallet to avoid credit card readers
- Use secured payments gateways like PayPal
- Put your attention to detail on websites or with email you are sent, look for grammar and spelling mistakes
- Be wary of any low-end hardware devices, many are not secure
- Do not click links sent to you on any device from untrusted contacts
- Educate your staff and family on cybersecurity safety
- Be mindful of store-bought IoT Smart devices, many are not secure
- In an enterprise environment do not setup every system with the same local account and password, you leave hackers with the ability to have lateral movement to gain access to more privileged accounts.
- Always cover your passwords or pin codes when entering them, there may be onlookers or cameras watching
- Avoid disclosing your employer or any other sensitive information on social media accounts
- Avoid selling old phones, computers or devices to strangers, information may be recoverable
- Always confirm who you are speaking with or ask for a callback phone number before disclosing any private information over the phone
- Do not post your email address in the public domain
- Do not re-use passwords
- Avoid storing copies of your passport, ID or other documents on your computer or phone
- Back up your data regularly
- Be cautious of devices you connect to your network or plug into your computer such as hard drives.
- Have passwords on your backed up data
- Keep your devices on you while traveling and not in your luggage or in your hotel room