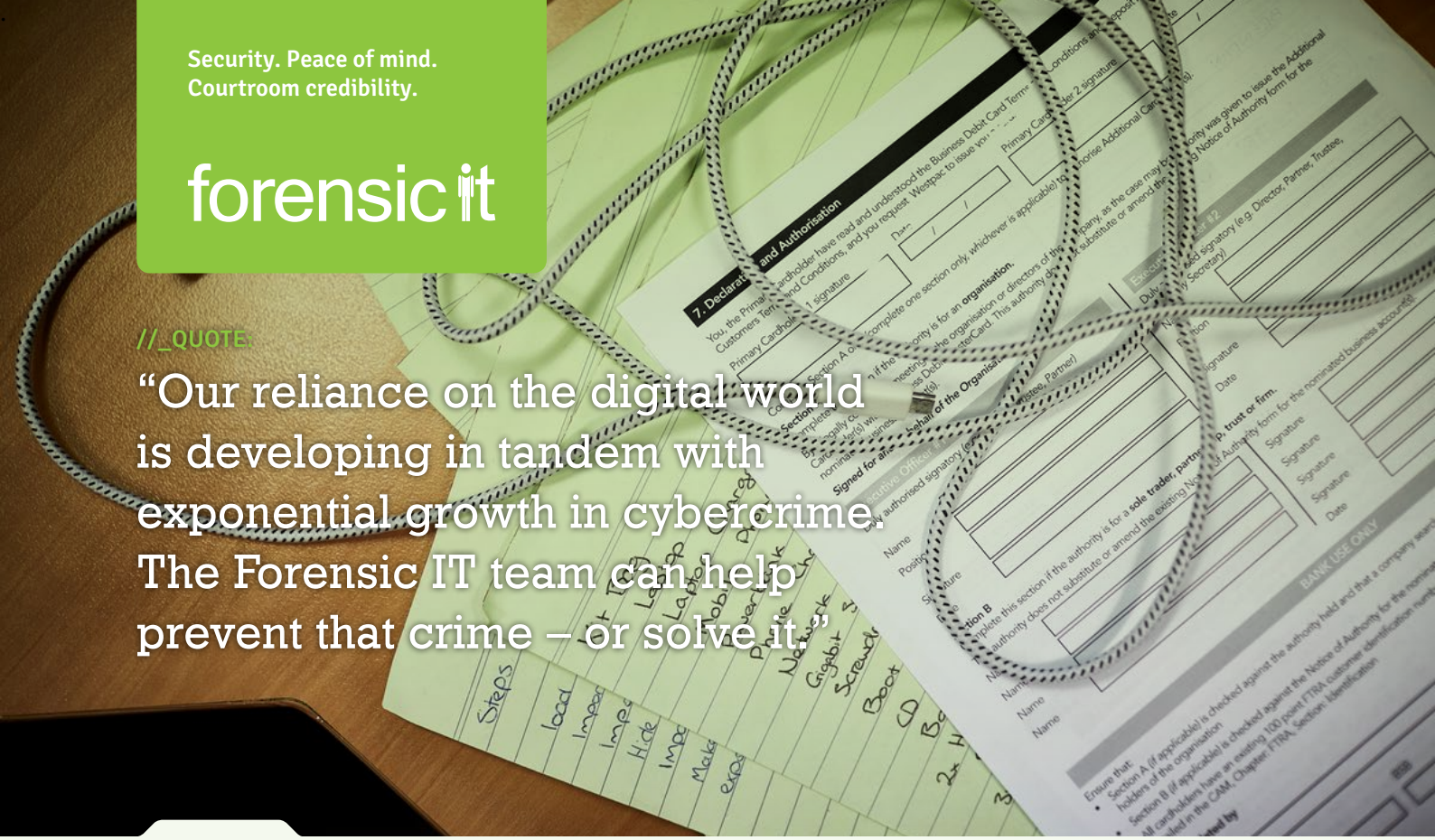
Security. Peace of mind.
Courtroom credibility.

forensic it



//_QUOTE:

“Our reliance on the digital world is developing in tandem with exponential growth in cybercrime. The Forensic IT team can help prevent that crime – or solve it.”

//_INTRODUCTION:

We are a team of highly qualified forensic IT specialists. We help our clients investigate crime and prevent crime. Our job is to make our clients’ businesses secure, to help them identify the culprits of cyber crime and prepare and present compelling evidence in court.

//_HOW WE CAN HELP:

If you believe the security of your business has been compromised, you need an expert who knows where to look to identify the crime, to preserve the evidence and find the culprit.

You need someone who understands courtroom procedure, with experience presenting complex evidence and a determination to deliver positive client outcomes.

At Forensic IT — that is what we do.

//_EXPERT SERVICES:

- System compromise investigations
- IT security
- Internet investigations
- Investigations into theft of intellectual property
- Mobile device extraction and analysis
- Fraud and financial investigations
- Covert data acquisition
- Forensic analysis
- Data preservation and recovery
- Search orders (Anton Piller)
- eDiscovery and litigation support
- Secure deletion
- Expert testimony
- Policy compliance review

//_BEST PRACTISE = BEST OUTCOME:

Organisations that employ best-practise digital security measures may not be impervious to attack, but they are significantly less likely to suffer system compromise.

Critically, if these organisations are the victims of system compromise, they are far better positioned to launch a forensic investigation.

When the Forensic IT team is called in, if the client has in place best-practise security measures, we know we are significantly more likely to find compelling evidence and deliver a positive outcome.

We advise our clients that the risk of:

- → **Spear Phishing** attacks can be minimised through use of two-factor authentication
- → **Interception of wireless networks** can be greatly reduced by using WPA2 encryption
- → **Losing critical digital evidence** can be overcome through regular email archiving
- → **System compromise** can be significantly reduced through password management software ensuring all staff utilise strong passwords

//_OUR APPROACH:

The Forensic IT team has unrivalled proficiency in the world of digital forensics. Our experience has taught us that there is no single technique for detecting cyber crime and no one-size-fits-all approach to preventing it.

Together, we have developed a vast toolkit of forensic analysis techniques. Our exhaustive investigative approach is underpinned by a commitment to thorough understanding of the underlying technology of modern software and IT devices.

This means we know where to look for evidence of changes to computer operating systems, where to seek tell-tale forensic artefacts that let us know someone has illegally infiltrated your network or accessed your valuable intellectual property.

We understand the potentially devastating effect cybercrime can have on a business or its reputation and we bring to the table the most effective methods for minimising the impact and reducing the risk of future attacks.

The Forensic IT team works with businesses, lawyers, investigators and government agencies to help wherever we can – whether it is through the identification of electronic evidence to support an investigation or through the production of clear and concise analysis for business or Court.

As one of the largest independent forensic IT service providers in Australia, we believe these services shouldn't cost the earth. It is our commitment to deliver the highest quality service at reasonable rates.

//_CONTACT FORENSIC IT TODAY:

ADDRESS: Level 18/114 William Street, Melbourne VIC 3000, Australia
PHONE: 03 9691 0804
EMAIL: enquiries@forensicit.com.au
WEBSITE: forensicit.com.au

forensic it