Fact sheet

BUSINESS CYBERCRIME

Business email compromise (BEC) is one of the fastest growing cybercrimes. BEC takes advantage of a gap in payment systems and using social engineering (psychological manipulation through technology) to dupe businesses into believing supplier bank account details have changed. This leads to a payment into the wrong account and an often devastating financial and reputational loss that is extremely difficult, if not impossible to recover.

Below is a guide on how you can help deter and prevent cybercrime in your business.

1. **Stay Aware** – keep up to date with the latest scams - attend cyber events, subscribe to security newsletters – then ensure your employees, colleagues and trading partners are aware by distributing new information regularly.
2. **Ensure security hygiene** – review your company practices in relation to password and security controls. Never share passwords across multiple sites or permit weak password. Use Multi-Factor Authentication (MFA) which is a two-step authentication of confirming a user's claimed identity for all systems where available including email.
3. **Recognise that employee email accounts are gateways** to highly sensitive information and attacks and therefore create and enforce policies restricting what information can be kept in email inboxes and for how long it should be kept before securely archiving it.
4. **Establish and enforce protocols in finance teams**. This could include protocols such as separation of duties and independent verification for changes to bank details. Do not trust or rely on emails for bank account changes – any change should be checked via a call back to the supplier using an independently sourced phone number.
5. **Ensure your systems are all running the latest security patches** and configured securely to remove or mitigate a threat.
6. **Use tools to enhance your security**. Spam filters and anti-virus software should be used and can prevent certain attacks. However, they don't work with the currently pervasive forms of scams such as BEC scams that use social engineering, rather than technological 'dark arts' to deceive people. Consider sourcing extra protection specifically designed identify and avoid BEC and payment scams. eftsure has a unique Know your Payee (KYP) payment protection solution that provides real-time alert signals (red thumbs and green thumbs) to businesses before they pay the wrong supplier. Powered by eftsure's live verified vendor database, they provide these alerts in online banking, or prior that, in an online portal.

To report actual or suspected criminal information, call 1800 333 000 or click nsw.crimestoppers.com.au

eftsure
www.eftsure.com.au

CRIME STOPPERS .com.au 1800 333 000

PARTNERS IN CYBERCRIME PREVENTION