CyberWardens.

20 July 2024

Media Release

Small business on guard against scam updates

Small businesses must be alert to phishing emails from scammers as the world reboots after the Microsoft-CrowdStrike outage.

Key points

1. Small business owners and employers should treat with suspicion any unexpected emails, screen pop-ups or phone calls purporting to come from Microsoft, CrowdStrike or large organisations such as banks and telcos.
2. Complete the fast free Cyber Wardens course this weekend to gain basic cyber security education before acting on any unsolicited or suspicious prompts to "reboot" or "update".
3. Go to Scamwatch.gov.au if you suspect you have been targeted by a scammer trying to access your computer.

Small businesses should review their digital security measures in the wake of the worldwide tech outage and take proactive steps to protect themselves and their clients, customers and communities.

COSBOA CEO Luke Achterstraat said in the wake of the CrowdStrike outage small businesses should prepare for an expected rise in cyber scammers exploiting the incident.

"We expect many small businesses will be targeted over the coming days by phishing and scammers with fake emails or phone calls with messages like 'I'm here to help you re-boot your system, just click here'," Mr Archterstraat said.

By clicking on a malicious link, scammers can steal passwords and install programs allowing them to have ongoing access to your computer.

The Australian Signal's Directorate's Australian Cyber Security Centre encourages all consumers to source their technical information and updates from official CrowdStrike sources only.

"It is crucial that businesses operate with heightened awareness after major outages or global events as attackers capitalise on our eagerness to resolve the issue or be better informed. We all need to slow down and think before we act as this will enable us to collectively better protect our customers," Matt Fedele-Sirotich, chief technology officer of CSO Group and Cyber Wardens advisor, said.

"While this incident was not a deliberate cyber attack, it underscores the importance of businesses taking proactive measures to mitigate the risk of such threats."

"Unfortunately it is often user error and lack of basic digital knowledge that opens the door to cyber threats, highlighting the need for ongoing education and awareness programs to strengthen cyber security resilience."

Protect yourself

STOP – Don't rush to act. Hang up on anyone asking you to download software or an app over the phone. Never provide banking information, passwords, or 2-factor identification codes over the phone.

THINK – Ask yourself if you really know who you are communicating with? Take the time to call the business you're dealing with using independently sourced contact details, or check you're talking to a real employee using their secure app.

PROTECT – Act quickly if something feels wrong. If you've shared financial information or transferred money, contact your bank immediately.

Source: National Anti-Scam Centre's Scamwatch

For more information, please visit cyberwardens.com.au

For media interviews please call 0409 994 433 or 0466 027 957 or email media@cyberwardens.com.au.

ENDS

Background

About Cyber Wardens

At Cyber Wardens, we are on a mission to ensure Australian small businesses operate in a cyber-safe environment.

By bolstering the cyber capabilities of people who work in small businesses, we make it easier for small businesses to increase their cyber posture to prevent attacks and be resilient to them. Our goal is simple — for cyber criminals to consider Australia 'closed for business'.

Cyber Wardens is a national initiative of the Council of Small Business Organisations of Australia (COSBOA), supported by the Australian Government and an industry alliance led by Telstra, CommBank and the Australian Cyber Security Centre, to help protect Australia's 2.5 million small businesses from online threats.