An Australian Government Initiative
Stay Smart Online

18 November 2016

Be wary of online scams as the holiday season approaches: Alert Priority Moderate

Scam emails that claim to come from reputable organisations are being sent to harvest personal details or to infect your computer with malicious software such as ransomware. Based on previous experience, email-based scams may increase during the 2016 holiday season.

In recent months, scammers have circulated fake email messages with malicious content that claim to be from the Australian Tax Office, AGL and Telstra. They have also used global brands such as PayPal to trick victims into providing personal details.

In many cases, scammers target these emails around events or deadlines that make the scam seem legitimate – such as the due date for submitting your business activity statements.

Shortly before Christmas 2015, the Australian Competition and Consumer Commission issued a warning about fake parcel deliveries that involved scammers taking advantage of the busy holiday season to send victims emails about 'missed parcel deliveries', purportedly from trusted services such as Australia Post or FedEx.

The ACCC said last year the scam emails may be personalised with individuals' names and addresses, and include logos from the company the emails claim to be from.

"The email may mention a fee will be charged while they hold your undelivered item," ACCC Deputy Chair Delia Rickard said at the time. "Scammers ask you to open an attachment or download a file to retrieve your parcel. If you follow these instructions, an executable file (.exe) will load on to your computer and install ransomware as soon as it is opened."

What is ransomware?
Ransomware is a type of malicious software that handicaps computer functionality, for example, through browser hijacking or encrypting personal data, and offers to restore the functionality for a fee, which is a form of extortion.

Recovery of systems that have been infected with ransomware is almost impossible without clean backups, so prevention is always the best approach.

While there have been reports that files are recovered if the ransom is paid, this does not protect your computer against further attacks. The attacker may simply encrypt your files again, and increase the ransom. For this reason, responding to extortion is not encouraged.

Staying safe

Prevention is the best antidote to ransomware and other malware attacks.

- Use spam filters and be cautious when opening emails, especially if there are attachments.
- Make sure you are using a reputable security software product.
- Make sure it is up-to-date and switched on.
- Make sure your operating system and applications are up-to-date and fully patched.
- Run a full scan of your computer regularly, or preferably set it to run automatically.
- Use strong and unique passwords.
- Set passwords on all your hardware devices (modems and routers) and change them regularly – never leave the default, factory set password in place – it is usually ‘admin’.
- Back up your data regularly.
- Keep a backup copy of your data in a safe place, disconnected from your computer and the internet, on a device that has been scanned.
- Only visit reputable websites and online services.