CLICK FRENZY= PHISHING FRENZY

mailguard

EMAIL SECURITY SOLUTIONS
WHITEPAPER

ARE YOUR STAFF SHOPPING ONLINE?
YOU HAVE A COMPANY-WIDE CYBERSECURITY ISSUE

Click Frenzy in November marks the start of online festive season shopping in Australia, followed by the global online shopping phenomena Black Friday. One-day pressure sales promise outrageous bargains from some of Australia's biggest retailers such as Myer, Sony, Bonds, and Air New Zealand. These sales encourage consumers *not* to think before they click—increasing the risk of being hooked by phishing scams.

Digital safety is not assured when shopping online

While it can be a great time to pick up a good deal before the rush, it's also an excellent time for phishing emails to circulate. If your staff are online shopping at work or accessing their private emails, they are making themselves vulnerable to cybercrime. It's not only their problem but also a company-wide issue.

Pressure tactics make the scene ripe for phishing

These type of one-day Click Frenzy sales put the onus on the customer to complete purchases as soon as possible, creating a huge sense of urgency, just in case they lose the deal to someone who was quicker to the mouse click or finger tap.

This is the exact tactic used in a phishing cybercrime scenario. The time critical tactic is a classic technique used to encourage targets to put aside their usual routine and checks for validity. Letting the drive for grabbing a bargain overtake common sense can be a fatal mistake.

If a person clicks through to an inbound phishing email purporting to be from a reputable online retailer but instead reaches a cloned website, the 'purchasing' of an item means scammers have just stolen their credit card and personal details. A hidden payload inside the 'online shopping' website may also be executed, resulting in compromised browser security and a whole computer system—including work data—to potentially fall victim to malicious intent.

The Click Frenzy one-day online sale shopping phenomena are modelled on Cyber Monday in the U.S., the biggest and most successful online U.S. sales event which grows significantly every year. 'Pressure shopping' means mindful consumer spending goes out the window. Cybercriminals capitalise on the same time-limited sale tactics that retailers use.

Be wary of parcel delivery and other sales scams

Other businesses besides online retailers may also be 'brandjacked' such as parcel delivery and banking services. 'Brandjacking' is a cybercrime term describing the act of hijacking a reputable company brand name in order to deceive and turn people into victims of cybercrime. Australia Post has just put out a similar bulletin about a scam email that looks to be from them, and last year a fake DHL email contained a trojan payload.

The facts on spending

Companies are budgeting for cybersecurity threats more than ever before, but those funds aren't always targeting the most significant dangers. Studies consistently show that the majority of cyberattacks are perpetrated via email, yet email security is often a low priority item in cybersecurity budgets.

On the consumer front, Australians have lost over $2.7m in online shopping scams this year to date in 2018 —and that's just what's been reported.

9 OUT OF 10 CYBERATTACKS START BY EMAIL

AUSTRALIANS HAVE LOST

IN ONLINE SCAMS THIS YEAR TO DATE IN 2018

1 IN 4 PEOPLE CLICK ON MALICIOUS CONTENT

> "Cybercrime is a serious and growing business risk. Building an effective cybersecurity culture within an organisation requires directors and executives to lead by example."
> *—Rob Sloan, Cybersecurity Research Director, Wall Street Journal*

5 tips for improving cybersecurity in your workplace

1

Always use a multi-layered approach for your business email security

This approach ensures additional coverage to deter phishing scammers and disable or quarantine likely hidden trojans in email messages.

2

Educate your team on how to spot a legitimate email address

Because email scams often look legitimate to the naked eye, education is key. Remind your staff how to spot a scam e.g. checking if the sender domain is legitimate and thinking before clicking links.

3

Keep your security services up-to-date

MailGuard’s Advanced Email Threat Protection provides zero-hour, real-time defense, giving immediate access to updates without the delay of downloading and testing a patch.

4

Make cybersecurity training in your company mandatory & continuous

As the cyberthreat environment constantly changes, so should your employee training. Commence training during employee on-boarding and continue throughout their tenure.

5

Audit your cybersecurity strategy and reporting procedures

If one of your employees receives a suspicious email, do they know how to deal with it and who they should report it to? Is your plan for dealing with malicious content up-to-date?

Learn more about strengthening your email security with MailGuard

Contact our cyber security experts now to protect your company from cybercrime

T 1300 30 44 30
E expert@mailguard.com.au