Cyber Security Threats & How Cyber Attacks Work

Council for Small Business Australia

Our Objective

- This presentation from COSBOA aims to introduce you to cyber security threats and how cyber attacks work.

- By the end of this presentation you will:
  - *be able to describe cyber security threats*
  - *understand how cyber attacks work*

What is a Cyber Attack?

- A cyber attack is *a deliberate effort to exploit digital systems*, from computers and networks, to mobile phones and websites.
- Cyber attackers make use of malicious coding to change the computer code, logic or data or the organisation or person they are attacking.
- Cyber attacks are aimed to be disruptive, causing a range of problems for those people who have been attacked.
- Consequences can include deleted, stolen or ransomed data, identity theft and are often disastrous for small businesses.

Types of Cyber Attacks

- Malware – malicious software that brings harm to a computer
- Viruses – a type of malware that attach to legitimate software
- Trojans – a file that looks normal but when accessed attacks the user
- Pharming – attempt to redirect website traffic to alternative site
- Phishing – attempt to gain private / sensitive information
- Ransomware – attempt to lock a system and demand ransom
- Spamming – attempt to send out unwanted digital messages
- Spoofing – attempt to send information pretending to be someone
- Spyware – attempt to infiltrate and then monitor to steal information

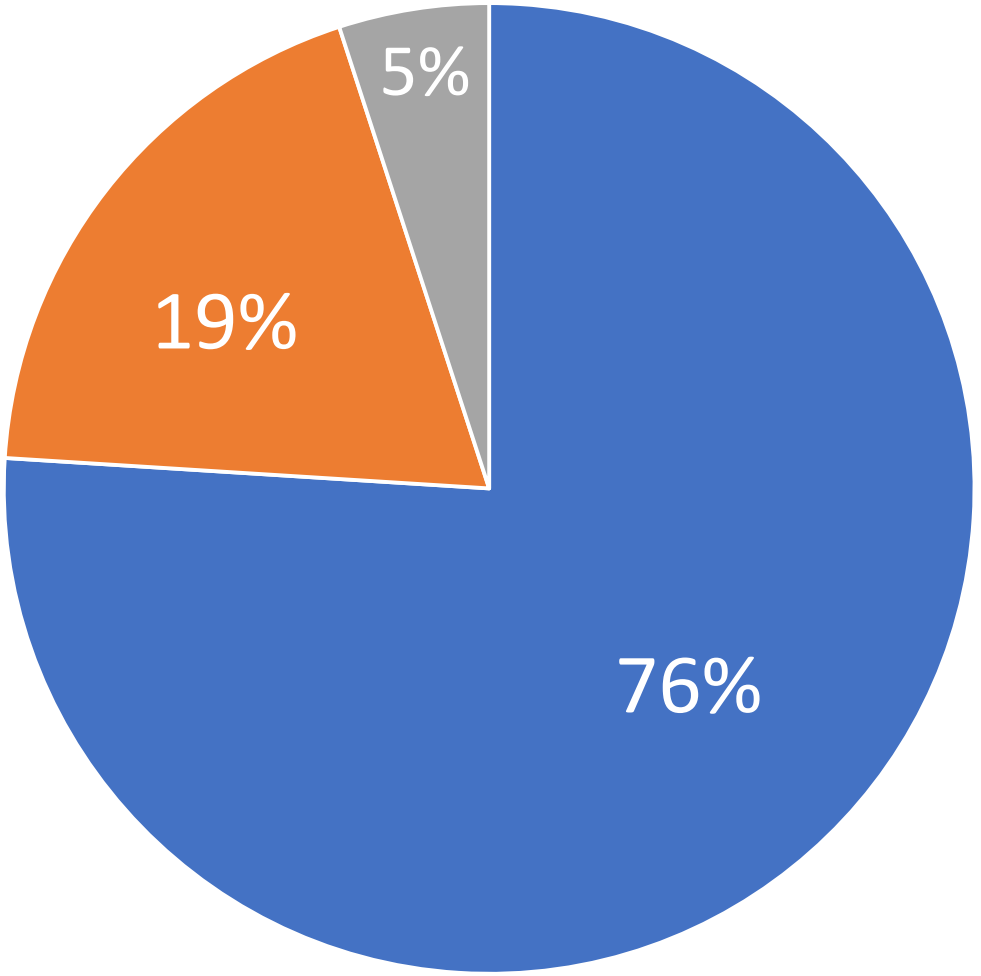
How does an Attack Work?

- Each cyber attack type has a different method, but most use imitation and other forms of trickery.
- Some attacks begin through the use of emails that seem real, attempting to trick the receiver and get them to do something.
- Other attacks attach their malware to files downloaded from websites or emails.
- Some attacks are through programs that you download for free, pretending to be something like a game but are actually intended to release malware.

Cyber Security Snapshot – Australia

- **1 in 5 small businesses** were impacted by a cyber attack in 2016.
- 11% of all small businesses were affected by ransomware.
- The average ransom paid by a small business was over $4,500
- 8% of owners who paid **did not get files back**.
- Average financial loss from each attack was over $6,500
- 24% of small businesses have **no cyber security software**.
- 41% of phones used for business have no cyber security software.
- 1/3 of all small businesses say they **would not last a week** without their critical information that can be locked by ransomware.
- 48% of small businesses **never back up their data**.
- 73% of survey respondents say they do not have cyber insurance.

Businesses affected by cyber attacks in Australia



YES – 76% NO – 19% UNSURE – 5%


There are many risks
in every small business

What Is At Risk In My Small Business?

- There are many different ways that criminals can target your small business.
- Devices such as phones, iPads, printers etc. are just as vulnerable as websites, computers, and Wi-Fi routers.
- Small businesses are at risk when their digital equipment and online presence is not protected.
- Protection is not just in the form of software, it includes actions and procedures that staff should be following.
- Even with protection, some criminals may gain access to your systems.

In Summary

- A **cyber attack** is a deliberate effort to exploit digital systems, from computers and networks, to mobile phones and websites.
- **Attacks work by** gaining access to the system of a small business through tricking a staff member into downloading or opening an email, or maliciously attacking a system.
- Other methods vary.
- **Small businesses in Australia are at a significant risk** – particularly when they do not manage cyber security threats.