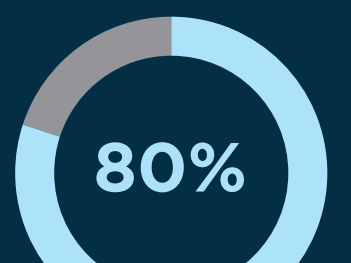
PROTECT YOUR BUSINESS FROM PHISHING SCAMS

What You and Your Staff Need to Know

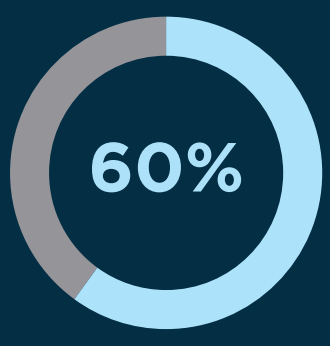
Phishing is the most common type of cybercrime.[1]

Knowledge Is Power

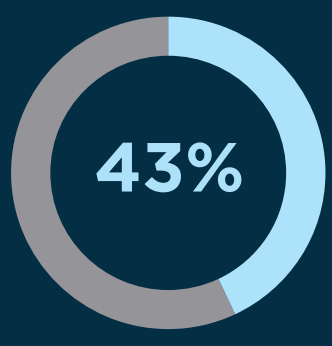
Phishing is a form of social engineering cybercriminals use to access your data. The scam typically begins with an email crafted to gain your trust. The goal is to trick you into clicking on a link (containing malware) or providing sensitive information (like a password).



of cybersecurity breaches are caused by human error[2]



of small businesses close within six months of a cyberattack[3]



of cyberattacks target small businesses[4]

Hackers attack every 39 seconds[5]

Cybersecurity Awareness 101

1

PAY CLOSE ATTENTION

Look at the sender's name and the URL. Read the email carefully. Do you see any misspellings or grammatical errors?

2

CONSIDER THE MESSAGE

Be suspicious of emails with urgent messaging and those requesting you provide sensitive information.

3

ERR ON THE SIDE OF CAUTION

When in doubt, never click on a suspicious link, open attachments or provide personal information.

Full-Scale Cybersecurity Protection Calls for a Multipronged Defense

Ensure networks, servers and devices are up to date

Block suspicious emails from your inbox with security filters

Rely on a solid backup and disaster recovery solution

Conduct regular cybersecurity awareness training

Knowledge is power and one of the most effective tools against social engineering scams. The more you and your staff know, the less likely cybersecurity attacks are to successfully infiltrate your business.

Sources:
[1]FBI, [2]IBM, [3]Inc., [4]Accenture, [5]University of Maryland

SMIKTECK

SMIKTECK PTY LTD
1300117645
https://www.smikteck.com.au
Suite 5/40 Harrison St,, Level 2
Cardiff, NSW 2285