OCTOBER 2022

dsp IT SOLUTIONS

TALKING TECH

HELPING YOUR BUSINESS

FROM DAMIEN'S DESK:

Here I am sitting in my son's apartment up in Townsville, it's school holidays so we try and get up to visit him when his tennis coaching is not so busy. Today is the national holiday in memory of the Queen, on the television and on social media there is news of our memorial service in Canberra for the monarch.

However, it's being over shadowed by the news that Optus (the telco) has been hacked, in the previous 24 hours. The US population are used to seeing this type of news specifically on a public holiday, peoples guards are down, staff are taking extra days to make a short week or long weekend. This is relatively new to us, but I suspect it is a continued sign of what is to come. More attacks, more frequently.

DID YOU KNOW?

Michael Dell (founder of Dell), Mark Zuckerberg (founder of Facebook) and Steve Jobs (founder of Apple) are all college dropouts.

This hack has not interrupted services or caused your mobile to go offline, it's not an attack on infrastructure. **In fact, it is a whole lot scarier than that.** The HACKERS stole **your** personal information and in coming days, months and even years it is going to be used against you. If you are a customer of Optus's then potentially the hackers now have you name, address, phone number, possibly even your date of birth and drivers licence number.

You are going to need to be super vigilant from today. The data that the hackers have could allow them to impersonate you, even open bank accounts in your name. There will be undoubtably a tirade of phishing emails coming your way to try and get access to the systems you use.

Here are two really import things you should do right now:

1. Make sure you have multifactor authentication turned on. This should be done on all systems that allow it, including your mobile phone – a passcode.
2. Regularly change your password. I would recommend using a password manager to help control your passwords and not use the same password everywhere.

If you would like us to complete a FREE Dark Web scan for you to see if any of your organisation's passwords are floating around the Dark Web please contact us using this form - https://www.dspit.com.au/contact-us/

Stay vigilant and safe out there.

Damien Pepper - Managing Director
dSP IT Solutions

dSP IT Solutions
182C Sladen Street
Cranbourne VIC 3977

HOW OFTEN DO YOU NEED TO TRAIN EMPLOYEES ON CYBERSECURITY AWARENESS?

You've just completed your annual phishing training where you teach employees how to spot phishing emails. You're feeling good about it, until about 5-6 months later when your company suffers a costly ransomware infection because someone clicked on a phishing link.

You wonder why you seem to need to train on the same information every year, and yet still suffer from security incidents. The problem is that you're not training your employees often enough. People can't change behaviours if training isn't reinforced regularly. They can also easily forget what they've learned after several months go by.

So, how often is often enough to improve your team's cybersecurity awareness and cyber hygiene? It turns out that training every four months is the "sweet spot" when it comes to seeing consistent results in your IT security.

It has been found that four months after employees receiving training, they were still able to accurately identify and avoid clicking on phishing emails.

However, after 6 months, their scores started to get worse. Then they continued to decline further the more months that passed after their initial training.

So, to keep employees well prepared to act as positive agents in your overall cybersecurity strategy, it's important they get training and refreshers regularly.

Tips on What & How to Train Employees to Develop a Cybersecure Culture

The gold standard for employee security awareness training is to develop a cybersecure culture. This is one where everyone is conscious of the need to protect sensitive data, avoid phishing scams, and keep passwords secured.

Unfortunately, this is not the case in most organisations. According to the 2021 Sophos Threat Report, one of the biggest threats to network security is a lack of good security knowledge and practices.

The report states, ***"A lack of attention to one or more aspects of basic security hygiene has been found to be at the root cause of many of the most damaging attacks we've investigated."***

Well-trained employees significantly reduce a company's risk of falling victim to any number of different online attacks.

To be well-trained doesn't mean you have to conduct a long day of cybersecurity training every four months. It's better to mix up the delivery methods.

Here are some examples of engaging ways to train employees on cybersecurity that you can include in your training plan:

· Self-service videos that get emailed once per month

· Team-based roundtable discussions

· Security "Tip of the Week" in company newsletters or messaging channels

· Training session given by an IT professional

· Simulated phishing tests

· Cybersecurity posters

· Celebrate Cybersecurity

· Awareness Month in October

*HOW USING THE **SLAM** METHOD CAN IMPROVE PHISHING DETECTION*

Why has phishing remained such a large threat for so long? Because it continues to work. Scammers evolve their methods as technology progresses, employing AI-based tactics to make targeted phishing more efficient.
If phishing didn't continue returning benefits, then scammers would move on to another type of attack. But that hasn't been the case. People continue to get tricked.

In May of 2021, phishing attacks increased by 281%. Then in June, they spiked another 284% higher.

Studies show that as soon as 6 months after a person has been trained on phishing identification, their detection skills can begin waning as they forget things.

Give employees a "hook" they can use for memory retention by introducing the SLAM method of phishing identification.

What is the SLAM Method for Phishing Identification?

One of the mnemonic devices known to help people remember information they are taught is the use of an acronym. SLAM is an acronym for four key areas of an email message that should be checked before trusting it.

These are:
S = Sender
L = Links
A = Attachments
M = Message text

By giving people the term "SLAM" to remember, it's quicker for them to do a check on any suspicious or unexpected email without missing something important.

All they need to do is run down the cues in the acronym.

S = *Check the* Sender

It's important to check the sender of an email thoroughly.

Often scammers will either spoof an email address or use a look-alike address that people easily mistake for the real thing.

L = *Hover Over* Links *Without Clicking*

Hyperlinks are popular to use in emails because they can often get past antivirus/anti-malware filters.

You should always hover over links without clicking on them to reveal the true URL.

This often can immediately call out a fake email scam due to them pointing to a strangely named or misspelled website.

A = *Never Open Unexpected or Strange File* Attachments

Never open strange or unexpected file attachments, and make sure all attachments are scanned by an antivirus/anti-malware application before opening.

M = *Read the* Message *Carefully*

If you rush through a phishing email, you can easily miss some telltale signs that it's a fake, such as spelling or grammatical errors.

Get Help Combatting Phishing Attacks

Both awareness training and security software can improve your defences against phishing attacks. Contact us today to discuss your email security needs.

ARE YOU A GOOD REMOTE LEADER?

We have reached a new age in the workplace. Back in the 1980s, business books and seminars encouraged managers to meander around the office, chat with colleagues and try to gather valuable information around the water cooler.

Now managers are working remotely, and it's a completely different world.

It's not always evident who the great leaders are in a remote setting, and you may have wondered at some point if you are even good at it. Truthfully, we don't have enough data yet to accurately evaluate what differentiates a great remote leader from the rest. But from my insights and experience running a fully remote company for 25 years, I've put together five questions that help determine if a remote leader is above average or not.

-Are you great at setting goals?
-Are you great at hiring?
-Are you great at delegating?
-Do you always do what you say you will do?
-Does your compensation system reward high performance?

If you can answer yes to all five of these questions, it's likely that you are a great remote leader.

These are essential leadership qualities for any setting, but they become amplified with remote work. If you set unclear goals in an office, you can easily clarify when your team has questions. This becomes more difficult when working remotely.

If you aren't great at hiring, you will notice these mistakes quickly in an office environment – but it's difficult to tell if you hired the wrong person in a remote setting. Additionally, you have to be great at delegating tasks and following up to make sure the work is being completed in a remote setting, because you can't physically see the process.

In a traditional office setting, peer pressure plays an impactful role in influencing your employees' behaviour. When you remove the peer pressure, compensation becomes the biggest driving force, so you need to make sure your compensation system is rewarding the right behaviour.

If you're wondering about the final question's role in an office, it's actually quite simple. You need to build and maintain trust in your workplace, and this becomes more difficult in a remote setting. That's why it's important that you always follow through on your words.

The remote workplace is here to stay, and it may take some adjustment to become the same caliber leader that you were in a traditional office setting. If you ask yourself those five questions every day and make the necessary adjustments in the categories you fall short in, before you know it, you'll become a great remote leader.

NEED A LAUGH?

What was the spider doing on the computer?

Making a web-site!

WIN A $30 VILLAGE GIFT CARD!

There was no winner to last month's trivia question. The answer was a) A video dating service

You could be the winner of this month's trivia, just contact us with the answer to the question below, Good Luck!

What is the world's best-selling PC game?
a) Minecraft
b) World of Warcraft
c) Half-Life 2
d) Doom

Call us with your answer (03) 9001 0817 or email jo@dspit.com.au