FROM DAMIEN'S DESK:

Some would say I am always banging on about Cybersecurity. There is a reason for that. It is extremely important, and all organisations should be looking to mitigate their exposure. The bad guys are after your data. Each day there are more and more attacks.

This is why in this month's newsletter we have put together an article on malware and what today's landscape looks like. The concern is that malware can be deployed without a user even clicking anything. I would encourage you to read the article and educate yourselves on some cost-effective protections that are available to any organisation.

Have you got remote or work from home users? Check out our Top 7 Cybersecurity Risks checklist on page three.

I am going to give you a heads up on a price rise coming shortly from Microsoft which will affect all Microsoft Office 365 users. Whilst Microsoft has not announced the exact price, I can tell you that as 1st September all Office 365 products will be increasing. There are some ways to lock in current pricing prior to the date, but you need to act now. Please reach out to arrange a time to discuss how we could lock in today's pricing for the next 12 months.

I am always open to having a coffee with anyone who wants to pick my brain, just reach out to me at damien@dspit.com.au and we will setup a time.

Stay safe out there

Damien Pepper - Managing Director
dSP IT Solutions

DID YOU KNOW ?

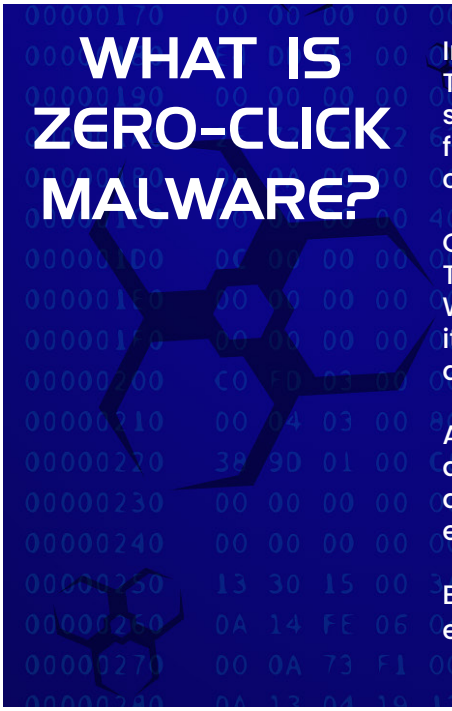
The first-ever email was sent in 1971 by computer engineer Ray Tomlinson.

For your FREE copy of this book, go to:
https://www.dspit.com.au/cybersecurity-essentials/

dSP IT Solutions
182C Sladen Street
Cranbourne VIC 3977
(03) 9001 0817
sales@dspit.com.au
www.dspit.com.au

#SuperResponsive #WeMakeTheComplexSimple #BuildRelationships #NothingIsTooHard

WHAT IS ZERO-CLICK MALWARE?



In today's digital landscape, cybersecurity threats continue to evolve. They pose significant risks to individuals and organisations alike. One such threat gaining prominence is zero-click malware. This insidious form of malware requires no user interaction. It can silently compromise devices and networks.

One example of this type of attack happened due to a missed call. That's right, the victim didn't even have to answer. This infamous WhatsApp breach occurred in 2019, and a zero-day exploit enabled it. The missed call triggered a spyware injection into a resource in the device's software.

A more recent threat is a new zero-click hack targeting iOS users. This attack initiates when the user receives a message via iMessage. They don't even need to interact with the message of the malicious code to execute. That code allows a total device takeover.

Below, we will delve into what zero-click malware is. We'll also explore effective strategies to combat this growing menace.

Understanding Zero-Click Malware

Zero-click malware refers to malicious software that can do a specific thing. It can exploit vulnerabilities in an app or system with no interaction from the user. It is unlike traditional malware that requires users to click on a link or download a file.

The Dangers of Zero-Click Malware

Zero-click malware presents a significant threat. This is due to its stealthy nature and ability to bypass security measures. Once it infects a device, it can execute a range of malicious activities.

These include:

· Data theft
· Remote control
· Cryptocurrency mining
· Spyware
· Ransomware
· Turning devices into botnets for launching attacks

This type of malware can affect individuals, businesses, and even critical infrastructure. Attacks can lead to financial losses, data breaches, and reputational damage.

Fighting Zero-Click Malware

To protect against zero-click malware, it is crucial to adopt two things. A proactive and multilayered approach to cybersecurity.

Here are some essential strategies to consider:

Keep Software Up to Date

Regularly update software, including operating systems, applications, and security patches. This is vital in preventing zero-click malware attacks. Software updates often contain bug fixes and security enhancements.

Put in Place Robust Endpoint Protection

Deploying comprehensive endpoint protection solutions can help detect and block zero-click malware. Use advanced antivirus software, firewalls, and intrusion detection systems.

Use Network Segmentation

Segment networks into distinct zones. Base these on user roles, device types, or sensitivity levels. This adds an extra layer of protection against zero-click malware.

Conduct Regular Vulnerability Assessments

Perform routine vulnerability assessments and penetration testing. This can help identify weaknesses in systems and applications.

Use Behavioural Analytics and AI

Leverage advanced technologies like behavioural analytics and artificial intelligence. These can help identify anomalous activities that may indicate zero-click malware.

cont'd P3

cont'd from P2

Educate Users
Human error remains a significant factor in successful malware attacks. Educate users about the risks of zero-click malware and promote good cybersecurity practices. This is crucial. Encourage strong password management. As well as caution when opening email attachments or clicking on unfamiliar links.

Uninstall Unneeded Applications
The more applications on a device, the more vulnerabilities it has. Many users download apps then rarely use them. Yet they remain on their device, vulnerable to an attack.

Only Download Apps from Official App Stores
Be careful where you download apps. You should only download from official app store.

TOP 7 CYBERSECURITY RISKS OF REMOTE WORK

Remote work has become increasingly popular in recent times. It provides flexibility and convenience for employees. But there are some drawbacks to working outside the office. It's crucial to be aware of the cybersecurity risks that come with remote and hybrid work.

Here are the top cybersecurity risks and tips on how employees and employers can address them.

1. Weak Passwords and Lack of Multi-Factor Authentication:
Employers should set up access management systems to automate the authentication process.

2. Unsecured Wi-Fi Networks:
To protect company data, remote teams should use a Virtual Private Network (VPN).

3. Phishing Attacks:
To defend against phishing attacks, be cautious when opening emails. Especially those from unknown sources. Avoid clicking on suspicious links. Verify the sender's email address.

4. Insecure Home Network Devices:
Many remote workers use smart devices that introduce vulnerabilities to their network. Ensure you change the default device passwords and keep them updated with the latest firmware.

5. Lack of Security Updates:
To mitigate this risk, enable automatic updates on devices and software whenever possible. Regularly check for updates.

6. Data Backup and Recovery:
Keep all company files backed up automatically to a central cloud location.

7. Insufficient Employee Training:
Remote workers should receive proper cybersecurity training. It helps them to understand security risks and best practices. Unfortunately, many companies neglect this aspect of cybersecurity. Organisations should provide comprehensive and ongoing cybersecurity training to remote workers.

HANDY TECH CHECKLIST FOR YOUR OFFICE OR HOME MOVE

Moving can be a chaotic and stressful time. Especially when it comes to handling your valuable technology. Whether you're relocating your office or home, it's essential to take extra care. Both with fragile items and when packing and moving your devices and other tech items.

To help you navigate this process smoothly, we've put together a handy checklist. Use this to help ensure your technology remains safe and sound during the move.

- Back-Up Everything
- Organise and Label Cables
- Pack Devices Carefully
- Remove Ink Cartridges and Batteries
- Take Photos of Cable Connections
- Pack Your Wi-Fi Equipment Separately
- Secure Fragile Screens
- Inform the Movers about Fragile Items
- Test Everything After the Move

7 ADVANTAGES OF A DEFENCE-IN-DEPTH CYBERSECURITY STRATEGY

Cybersecurity threats are becoming increasingly sophisticated and prevalent.

A defence-in-depth cybersecurity strategy provides a strong and resilient defence system. It's several layers of security increase the chances of staying secure. This is especially important in today's dangerous online world.

Here are the Advantages of Adopting a Defence-in-Depth Approach:

1. Enhanced Protection
2. Early Detection and Rapid Response
3. Reduces Single Point of Failure
4. Protects Against Advanced Threats
5. Compliance and Regulatory Requirements
6. Flexibility and Scalability
7. Employee Education and Awareness

WE LOVE REFERRALS . .

The greatest gift anyone can give us is a referral to your business colleagues/ friends. Referrals help us keep costs down so we can pass the savings on to our clients. Simply introduce me via email to damien@dspit.com.au or (03) 9001 0817 and I'll take it from there.

NEED A LAUGH?

How did the man get a job at Microsoft's office?

Because he Excel-led in the interview!

WIN A $20 BUNNINGS GIFT CARD!

The winner of last month's trivia question was Ann from Showtime Attractions. The answer was d) Jumpman.

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

Mozilla Firefox originally launched under what name?

a) Mozilla Red Panda
b) Mozilla Firebird
c) Mozilla Firefly
d) Mozilla Phoenix

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