TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

Monthly update from Mark

Despite knowing better, many companies and individual PC users don't keep their systems and applications updated properly. While it may seem okay to click "later" on an update notification, let's be real... everyone gets busy doing other things, and that update often goes months without getting installed.

How do we know installing updates and security patches is such a big problem? A recent report from Tetra Defense found that in Q1 of 2022, 82% of cyberattacks on US organisations were the result of preventable unpatched vulnerabilities.

This means that had those companies simply kept up with their updates, attacks would have been just a fraction of what they were. Imagine going through a major ransomware attack costing you tens of thousands of dollars when it all could have been avoided if someone clicked "update now" instead of ignoring it.

While keeping all your systems updated sounds easy in theory, we realise that the more computers, tablets, servers, and other devices you get, the more complex it becomes to ensure they're all updated all the time. That's where automation comes in.

Automated patch and update management can keep your network from being a sitting duck for hackers and ease the burden of updating software constantly. Automatic patch management is what we do for all our Managed IT clients.

If you need help automating your updates to reduce the risk of a breach, just let us know. We'd love to chat. Drop us an email at mark@phrixus.com

Until then, stay safe,

Mark

DID YOU KNOW?

Twitter's original 140 character limit was due to it being originally built for SMS which only allow 160 characters (140+twitter handle with a 20 character limit)

Phrixus Technologies

PO Box 266
Berowra NSW 2081
www.phrixus.com
02 9457 6416

02

SMALL BUSINESSES ARE ATTACKED BY HACKERS 3X MORE THAN LARGER ONES

Small Businesses Are Attacked by Hackers 3x More than Larger Ones

Have you felt more secure from cyberattacks because you have a smaller business? Maybe you thought that you couldn't possibly have anything that a hacker could want? Didn't think they even knew about your small business.

Well, a new report out by cyber-security firm Barracuda Networks debunks this myth. Their report analysed millions of emails across thousands of organisations. It found that small companies have a lot to worry about when it comes to their IT security.

Barracuda Networks found something alarming. Employees at small companies saw 350% more social engineering attacks than those at larger ones. It defines a small company as one with less than 100 employees. This puts small businesses at a higher risk of falling victim to a cyberattack. We'll explore why below.

Why Are Smaller Companies Targeted More?

There are many reasons why hackers see small businesses as low-hanging fruit. And why they are becoming larger targets of hackers out to score a quick illicit buck.

Small Companies Tend to Spend Less on Cybersecurity

When you're running a small business, it's often a juggling act of where to prioritise your cash. You may know cybersecurity is important, but it may not be at the top of your list. So, at the end of the month, cash runs out, and it's moved to the "next month" wish list of expenditures.

Small business leaders often don't spend as much as they should on their IT security. They may buy an antivirus program and think that's enough to cover them. But with the expansion of technology to the cloud, that's just one small layer. You need several more for adequate security.

Hackers know all this and see small businesses as an easier target. They can do much less work to get a payout than they would trying to hack into an enterprise corporation.

Every Business Has "Hack-Worthy" Resources

Every business, even a 1-person shop, has data that's worth scoring for a hacker. Credit card numbers, SSNs, tax ID numbers, and email addresses are all valuable. Cyber-criminals can sell these on the Dark Web. From there, other criminals use them for identity theft.

Here are some of the data that hackers will go after:

- Customer records
- Employee records
- Bank account information
- Emails and passwords
- Payment card details

Small Businesses Can Provide Entry Into Larger Ones

If a hacker can breach the network of a small business, they can often make a larger score. Many smaller companies provide services to larger companies including digital marketing, website management, accounting, and more.

Vendors are often digitally connected to their client's systems.

This type of relationship can enable a multi-company breach. While hackers don't need that connection to hack you, it is a nice bonus.

Small Business Owners Are Often Unprepared for Ransomware

Ransomware has been one of the fastest-growing cyberattacks of the last decade. So far in 2022, over 71% of surveyed organisations experienced ransomware attacks.

The percentage of victims that pay the ransom to attackers has also been increasing. Now, an average of 63% of companies pay the attacker money in hopes of getting a key to decrypt the ransomware.

YUBIKEY

The world's #1 multiprotocol security key

The YubiKey 5 Series eliminates account takeovers by providing strong phishing defense using multi-protocol capabilities that can secure legacy and modern systems.

The series provides a range of authentication choices including strong two-factor, multi-factor and pass-wordless authentication, and seamless touch-to-sign.

Find yours at https://www.yubico.com/

03 THE BIGGEST VULNERABILITIES THAT HACKERS ARE CURRENTLY EXPLOITING

Software vulnerabilities are an unfortunate part of working with technology.

A developer puts out a software release with millions of lines of code. Then, hackers look for loopholes that allow them to breach a system through that code.

The developer issues a patch to fix the vulnerability. But it's not long before a new feature update causes more.

It's like a game of "whack-a-mole" to keep your systems secure.

Without ongoing patch and update management, company networks are vulnerable. And these attacks are completely avoidable.

82% of U.S. cyberattacks in Q1 of 2022 were due to exploiting patchable vulnerabilities.

What new vulnerabilities are lurking in products from Microsoft, Google, Adobe, and others?

We'll go through several. These were recently noted in a warning by the Cybersecurity and Infrastructure Security Agency (CISA).

Make Sure to Patch Any of These Vulnerabilities in Your Systems

Microsoft Vulnerabilities

- CVE-2012-4969: An Internet Explorer vulnerability that allows the remote execution of code.
- CVE-2013-1331: This Microsoft Office flaw enables hackers to launch remote attacks.
- CVE-2012-0151: This Windows vulnerability allows user-assisted attackers to execute remote code.

Google Vulnerabilities

- CVE-2016-1646 & CVE-2016-518: These Chrome & Chromium engine vulnerabilities both allow attackers to conduct denial of service attacks.

Adobe Vulnerabilities

- CVE-2009-4324: This is a flaw in Acrobat Reader that allows hackers to execute remote code via a PDF file.
- CVE-2010-1297: A Flash Player vulnerability that allows remote execution and denial of service attacks. (Flash Player is no longer supported, so you should remove it).

Netgear Vulnerability

- CVE-2017-6862: This router flaw allows a hacker to execute code remotely.

Cisco Vulnerability

- CVE-2019-15271: This vulnerability impacts Cisco RV series routers, and gives a hacker "root" privileges.

Patch & Update Regularly!

These are a few of the security vulnerabilities listed on the CISA list. You can see all 36 that were added at https://www.cisa.gov

How do you keep your network safe from these and other vulnerabilities?

You should patch and update regularly. Work with a trusted IT professional (like us) to manage your device and software updates.

This ensures you don't have a breach waiting to happen lurking in your network.

04 WHAT IS MICROSOFT DEFENDER FOR INDIVIDUALS?

When you hear about Microsoft adding security apps to M365, it's often the business versions.

But the pandemic has changed the way that we see the workplace.

It's now a world made up of several connected "mini-offices" located in employee homes.

55% of employees use their own devices and software to work from home. For most organisations these are non compliant.

The latest security offering by Microsoft is not for business plans.

It's for Personal and Family users of Microsoft 365.

The Basics of Microsoft Defender for Individuals

Microsoft Defender is a new app that Microsoft 365 subscribers can download.

It brings many digital protections together into one dashboard.

These include the following:

Online Security Visibility

Microsoft Defender gives you visibility into the security status of all your devices.

Device Safeguards

The app includes extra protections from online threats.

Real-Time Alerts & Recommendations

It provides real-time alerts for security. These also come with recommended actions.

What Devices Can Use It?

- Windows: Windows 10 version 19041.0 and higher
- Mac: Intel Macs from Catalina 10.15 and higher, and Apple silicon-based devices from 11.2.3 and up
- iPhone: iOS 13.0 or later
- Android: Android OS 6.0 or later

05 5 MISTAKES COMPANIES ARE MAKING IN THE DIGITAL WORKPLACE

The pandemic has been a reality that companies around the world have shared. It required major changes in how they operate. No longer, did the status quo of having everyone work in the office make sense for everyone. Many organisations had to quickly evolve to working through remote means.

Overcoming the challenges and reaping the benefits takes time and effort. It also often takes the help of a trained IT professional, so you avoid costly mistakes such as:

- Poor Cloud File Organisation
- Leaving Remote Workers Out of the Conversation
- Not Addressing Unauthorised Cloud App Use
- Not Realising Remote Doesn't Always Mean From Home
- Using Communication Tools That Frustrate Everyone

06 SAVE RECURRING EMAIL TEXT IN OUTLOOK'S QUICK PARTS

Do you have certain emails you send to customers that have the same paragraphs of text in them?

For example, it might be directions to your building or how to contact support.

Stop retyping the same info every time.

Outlook has a feature called Quick Parts that saves and then inserts blocks of text into emails.

- Create a Quick Part by highlighting the text to save in an email.
- On the Insert Menu, click Quick Parts.
- Save Quick Part.

When ready to insert that text into another email, just use the same menu.

Then click to insert the Quick Part.

07 INTERNET EXPLORER HAS LOST ALL SUPPORT (WHAT YOU NEED TO KNOW)

After being the main entry to the internet in the late 1990s and early 2000s, Internet Explorer (IE) is gone. As of June 15, 2022,Microsoft dropped the web browser from support.

To ease the transition away from Internet Explorer, Microsoft added IE Mode to Edge. This mode makes it possible for organisations to still use legacy sites that may have worked best in IE. It uses the Trident MSHTML engine from IE11 to do this.

If you haven't yet addressed old copies of IE on your computers, your network could be at risk due to vulnerabilities in the browser no longer being fixed. Here's what you should do:

1. Migrate Browser Data to Microsoft Edge from IE
2. Uninstall the IE Browser
3. Ensure Employees Know How to Use IE Mode in Edge
4. Train Employees on Microsoft Edge Features

WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to your friends. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll gift them their free first month of service (for being a friend of yours) AND we'll gift you $500 cash/gift voucher.
Simply introduce me via email to mark@phrixus.com and I'll take it from there. I personally promise we'll look after their business with a high level of care and attention (just like we do with all our clients).

NEED A LAUGH?

What sound does a mouse make?

Click?

TECHNOLOGY TRIVIA

Each month you have a chance to win a $50 Amazon Gift Voucher by being the first person to email us with the answer to our Technology Trivia Question of the Month!

The question this month is:

What do you call a company's internal network?

The first person to email me at **mark@phrixus.com** and give a correct answer gets a $50 Amazon Gift Card! Well done to Geraldine for being the only correct answer received last month

Email Daily quarantine report

We often receive requests to increase the frequency of the daily quarantine report in M365. Whilst the automated delivery cannot be increased to more than once per day you can access the end user quarantine anytime without having to wait for the daily report, save the following URL in your favourites:

https://security.microsoft.com/quarantine

AzureAD joined systems should login automatically but if you are prompted to login, use your Microsoft 365 credentials.

You will then be logged into the quarantine page as below, from here you can check all emails captured by the filter and release any false positives you are CERTAIN are safe.

News from the Phrixus Team

We congratulate Mark on his marriage to Sarah on Oct 1st and also to Rob on his marriage to Lauren on Oct 8th. Rob will be taking a few weeks off with his new bride. We wish them the best of luck and hope the rain stays away.