TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

Monthly update from Mark

We know that most work is done in the cloud these days. For some types of software, you are hard-pressed to even find an on-premises version. What does this mean for your company's data security? It means that how you manage identities and logins matters a lot.

If you're still using a simple username & password combination to grant access to business accounts, you may want to rethink that. Passwords are notorious for being hacked, as well as being released on the dark web after a breach.

There are more solutions available to you these days. Including contextual multi-factor, single sign-on, passkeys, and more. If you'd like to explore your options, email us at mark@phrixus.com to schedule a chat.

Until then, stay safe,

Mark

DID YOU KNOW

The first known computer programmer was a woman named ADA LOVELACE

Phrixus Technologies

PO Box 266
Berowra NSW 2081
www.phrixus.com

02 9457 6416

IS IT TIME TO DITCH THE PASSWORDS FOR MORE SECURE PASSKEYS?

02

Passwords are the most used method of authentication, but they are also one of the weakest. Passwords are often easy to guess or steal. Also, many people use the same password across several accounts. This makes them vulnerable to cyber-attacks.

The sheer volume of passwords that people need to remember is large. This leads to habits that make it easier for criminals to breach passwords. Such as creating weak passwords and storing passwords in a non-secure way.

61% of all data breaches involve stolen or hacked login credentials.

In recent years a better solution has emerged – passkeys. Passkeys are more secure than passwords. They also provide a more convenient way of logging into your accounts.

What is Passkey Authentication?

Passkeys work by generating a unique code for each login attempt. This code is then validated by the server. This code is created using a combination of information about the user and the device they are using to log in.

You can think of passkeys as a digital credential. A passkey allows someone to authenticate in a web service or a cloud-based account. There is no need to enter a username and password.

This authentication technology leverages Web Authentication (WebAuthn). This is a core component of FIDO2, an authentication protocol. Instead of using a unique password, it uses public-key cryptography for user verification.

The user's device stores the authentication key. This can be a computer, mobile device, or security key device. It is then used by sites that have passkeys enabled to log the user in.

Advantages of Using Passkeys Instead of Passwords

More Secure

One advantage of passkeys is that they are more secure than passwords. Passkeys are more difficult to hack. This is true especially if the key generates from a combination of biometric and device data.

Biometric data can include things like facial recognition or fingerprint scans. Device information can include things like the device's MAC address or location.

This makes it much harder for hackers to gain access to your accounts.

More Convenient

Another advantage of passkeys over passwords is that they are more convenient. With password authentication, users often must remember many complex passwords. This can be difficult and time-consuming.

Forgetting passwords is common and doing a reset can slow an employee down. Each time a person has to reset their password, it takes an average of three minutes and 46 seconds.

Passkeys erase this problem by providing a single code. You can use that same code across all your accounts. This makes it much easier to log in to your accounts.

It also reduces the likelihood of forgetting or misplacing your password.

Phishing-Resistant

Credential phishing scams are prevalent. Scammers send emails that tell a user something is wrong with their account.

They click on a link that takes them to a disguised login page created to steal their username and password.

When a user is authenticating with a passkey instead, this won't work on them. Even if a hacker had a user's password, it wouldn't matter. They would need the device passkey authentication to breach the account.

03 HOW TO CREATE INSIGHTFUL DASHBOARDS IN MICROSOFT POWER BI

Data visualisation is a powerful tool for communicating complex data.

But it is not enough to simply create a graph or chart and call it a day. To truly make use of information, it is important to create insightful reports.

Creating holistic and insightful reports requires the use of several data points. One tool that enables this is Microsoft Power BI.

What Is Microsoft Power BI?

Microsoft Power BI is a business intelligence tool. It allows you to connect many data sources to one dashboard. Using Power BI, you can easily model and visualise data holistically.

Tips for Designing Great Data Visualisation Reports

Consider Your Audience

You should design reporting dashboards with the end user in mind.

CEOs and CFOs are interested in different aspects of the business, make the information interesting to them.

- What is it that this audience wants to see?
- Are they looking for bottomline sales numbers?
- Or do they want to cover insights that can help target productivity gaps?

Don't Overcomplicate Things

Many times, less is more. If you find that your dashboard looks crowded, you may be adding too many reports.

The more you add, the more difficult it is to read the takeaways from the data.

Try Out Different Chart Types

Experiment with presenting your data in different ways.

Flip between bar, pie, and other types of charts to find the one that tells the story the best.

Just don't go overboard. Keep it simple but interesting.

Get to Know Power Query

Power Query is a data preparation engine.

- Take time to learn how to leverage this tool for help with:
- Connecting a wide range of data sources to the dashboard
- Previewing data queries
- Building intuitive queries over many data sources
- Defining data size, variety, and velocity

Build Maps with Hints to Bing

Bing and Power BI integrate, allowing you to leverage default map coordinates. Use best practices to utilise the mapping power of Bing to improve your geo-coding.

Tell People What They Are Looking At

A typical comment heard often when presenting executives with a new report is, "What am I looking at?" Tell your audience what the data means by using features like tooltips and text boxes to add context.

Use Emphasis Tricks

People usually read left to right and from top to bottom. So put your most important chart at the top, left corner. Follow, with the next most important reports.

04 WHAT IS PUSH-BOMBING & HOW CAN YOU PREVENT IT?

Cloud account takeover has become a major problem for organisations.

Between 2019 and 2021, account takeover (ATO) rose by 307%. Many organisations use multi-factor authentication (MFA) as a way to stop fraudulent sign-ins.

But its effectiveness has spurred workarounds by hackers. One of these is push-bombing.

How Does Push-Bombing Work?

When a user enables MFA on an account, they typically receive a code or authorisation prompt of some type.

The user enters their login credentials.

Then the system sends an authorisation request to the user to complete their login.

With push-bombing, hackers start with the user's credentials and take advantage of that push notification process.

They attempt to log in many times.

This sends the legitimate user several push notifications, one after the other.

When someone is bombarded with these, it can be easy to mistakenly click to approve access.

Push-bombing is a form of social engineering attack designed to:

- Confuse the user
- Wear the user down
- Trick the user into approving the MFA request to give the hacker access

Ways to Combat Push-Bombing at Your Organisation

- Educate Employees
- Reduce Business App "Sprawl"
- Adopt Phishing-Resistant MFA Solutions
- Enforce Strong Password Policies
- Put in Place an Advanced Identity Management Solution

Additionally, businesses can use identity management solutions to install contextual login policies.

05 HOW TO USE CHATGPT AT YOUR BUSINESS RESPONSIBLY

ChatGPT has revolutionised the way businesses interact with their customers. It has also affected how they get things done.

Teams are using it for everything from emails to generating ideas for product names.

The tool's personalised and informative responses in real-time definitely draw you in. But integrating ChatGPT into your business operations requires careful consideration.

You want to ensure that things don't get out of hand with employees using the tool irresponsibly.

- Understand ChatGPT's Weaknesses
- Define ChatGPT's Role
- Consider Customer Privacy
- Ensure Human Oversight
- Integrate ChatGPT Into Your
- Existing Customer Service
- Measure Performance and Optimise
- Be Transparent About Using It

06 7 WAYS TO SECURE YOUR WIRELESS PRINTER

Many people worry about someone hacking their computer. But they're not really thinking about their wireless printer getting breached. It's a tool that most individuals use sporadically. For example, when you want to print out tax forms or mailing labels.

Printers tend to be out of sight, out of mind. That is until you need to print something and run out of ink. Well, they're not out of the mind of hackers. In fact, unsecured printers are a classic way for criminals to gain access to a home network.

1. Change the Default Login Credentials
2. Keep Printer Firmware Updated
3. Use a Network Firewall
4. Put Your Printer on a Guest Network
5. Disable Unused Ports or Services
6. Unplug It When Not in Use
7. Teach Your Family Cybersecurity Best Practices

07 6 IMMEDIATE STEPS YOU SHOULD TAKE IF YOUR NETFLIX ACCOUNT IS HACKED

Netflix is one of the most popular and well-known streaming services. The platform has become an essential part of many people's daily entertainment routines. Unfortunately, like any online service, Netflix accounts can be vulnerable to hacking.

Hackers take advantage of "phishing overload." Once they breach your account, they're usually quiet for a bit, hoping you'll mistake the Netflix suspicious login warning for a fake.

Here are some things to do right away if you fear your account is hacked:

1. Go to the Netflix site & try to log in.
2. If you can log in, change your password immediately.
3. If you can log in, remove any strange payment methods
4. Contact Netflix support and let them know that you think you've been compromised. (Don't skip this step)
5. Watch your bank statements.
6. Change the password for other accounts that used the same one as your Netflix account.

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).

Why Organisations should NEVER allow Employees to use the Default Mobile Phone Mail App

Organisations should REQUIRE their employees to ONLY use the Microsoft Outlook App on their mobile devices and here's why...
When a user uses the native Mail apps on their phones, all corporate emails, contacts, and calendar content synchronises with the Mail app
When the user launches some other app (like Uber, Facebook, WhatsApp, SnapChat), the app asks for permission to access the user's contacts and calendar appointments.
Users simply tap CONTINUE to give the mobile app / social media company full permission to now UPLOAD your company global address list (including ALL employee names, email addresses, mobile phone numbers, titles, etc (whatever you have in your Global Address list)) from the user's phone up to the 3rd party vendor.
How the Microsoft Outlook app differs is, when your user connects to Office 365 using the Microsoft Outlook mobile app, ALL emails, contacts, and calendar appointments remain **INSIDE** the Outlook app.
The user will NOT have your company address book, phone numbers, etc replicated into the normal "contacts" on their phone, thus when they tap to allow other mobile apps access to their contacts, your business address book will not be compromised.

Please always make sure as part of your company policies that you ensure staff ONLY use the Microsoft Outlook Application.

NEED A LAUGH?

Why did the computer go to art school?

Because it wanted to learn how to draw better "bytes"!

TECHNOLOGY TRIVIA

The question this month is:

Why does your keyboard have that weird QWERTY layout?

The first person to email me at **mark@phrixus.com** and give a correct answer gets a $50 Amazon Gift Card!

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!

MFA Authentication App - The correct one to use.

We have had a few cases where clients have downloaded the wrong Authenticator app for their Microsoft 365 security. Although our technicians always insist on you all using this one for the Microsoft security as it has more built in security features, there have been cases where the wrong one has been installed.
Please always be careful to follow our technicians instructions and if you have installed the wrong one and it is asking you to pay any money then you have the wrong one.
The Google Authenticator app can be used for all other MFA requirements but always use the Microsoft app for Microsoft security.