FROM DAMIEN'S DESK:

Well, this is it, the last month of this financial year. Do you need to put the pedal to the floor to hit the targets or goals you set 11 months ago?

Now is the time to take advantage of the instant asset write off. If you are a business with an aggregated turnover of less than $10 million, you can immediately deduct the total cost of eligible assets costing less than $150,000 if it is ready for use by 30th June 2023. This does include computers, servers and peripherals. If you need help sourcing and installing new devices, please contact us on (03) 9001 0817.

Artificial intelligence (AI) is now accessible by all internet savvy computer users. In the past, you have seen it in things like the pop-up chatbots or predictive text. Well now you can access AI to help you do almost anything. Check out chat.openai.com (ChatGPT). Send it a message and be gobsmacked with its reply. I just asked it "*How are you today*" and its reply was - *"As an AI language model, I don't have feelings in the way humans do, but I'm functioning properly and ready to assist you with any questions or tasks you may have. How can I assist you today?"*
This system has some great uses, but remember it's probably just a starting point, a first draft or a reference check. When you have writer's block, give ChatGPT the key ingredients and see what it can produce for you.

Stay safe out there

Damien Pepper - Managing Director
dSP IT Solutions

DID YOU KNOW?

Google receives over 99,000 search results every single second!

follow Us

Do you follow us on facebook?

Go to:
https://www.facebook.com/DSP.IT.Solutions.Managed.ITSupport.Melbourne

Like our page and follow us for links to informative articles

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

#SuperResponsive #WeMakeTheComplexSimple #BuildRelationships #NothingIsTooHard

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

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.

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.

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 usesporadically. For example, when you want to print out 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

TECHNOLOGIES TO GIVE YOU AN ADVANTAGE

Customers look for convenience. In today's world that means technology that makes their life easier.

From webforms to POS systems, you need to keep the customer experience in mind in all you do.

When people aren't happy with their experience interacting with a company, they leave.

And their experience might not have anything to do with your products or services. Maybe they found it hard to navigate your website.

Technology is key to converting website visitors into clients.

These technologies can give you that edge:
- Cloud Forms
- Digital Signatures
- Smart Chatbot
- SMS Notifications
- Business Mobile App
- FAQ Kiosk
- VoIP Phone System

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
- Measure Performance and Optimise
- Be Transparent About Using It
- Integrate ChatGPT into your Existing Customer Service

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?

Why did the computer show up at work late?

It had a hard drive!

WIN A $20 BUNNINGS GIFT CARD!

The winner of last month's trivia question was Tony from Unique Building Services.
The answer was a) A paper manufacturer in 1865.

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

In what video game series did Microsoft's virtual assistant Cortana make her debut?

a) Forza
b) Halo
c) Age of Empires
d) Battlefield

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