AUGUST 2025

Your monthly newsletter, written for humans not geeks

TECHNOLOGY INSIDER

Could social engineering **bring down your business?**

One phone call could be all it takes to bring your business to its knees.

That's the chilling reality of social engineering. It's a type of cyberattack that doesn't rely on clever coding or fancy tech. Instead, it targets your people. And it's becoming one of the biggest threats to businesses of all sizes.

Social engineering is when a criminal manipulates someone into giving up sensitive information or access to systems. It often starts with a phone call or email from someone pretending to be a colleague, a supplier, or even a senior manager. They might sound friendly, urgent, or frustrated… anything to get the response they want.

And if your staff aren't on high alert, that one conversation could open the door to your entire network.

A favorite target for these attacks?

Your help desk or service team. They're trained to be helpful and solve problems quickly. But if someone calls pretending to be locked out of their account and urgently needs a password reset, it's easy to see how a well-meaning team member could be tricked into handing over access.

From there, it's game over. Attackers can install ransomware, steal customer data, or snoop around in your systems undetected.

The worst part is this kind of attack is simple to pull off. And highly effective. That's why even small businesses need to take it seriously.

So, what can you do?

Start by training your team to be cautious of unusual requests, even if they sound legitimate. And don't rely on memory or gut instinct. Put strong identity verification procedures in place that everyone follows, every time. Technology can help with this, by adding extra checks before any sensitive action is taken.

Remember, cybercriminals don't need to break in when someone will open the door for them. But with the right awareness and safeguards, you can make sure your team knows how to keep it firmly shut.

Need help keeping your team on top of cyber security best practice? Get in touch.

DID YOU KNOW…

not all password managers are genuine?

Cybercriminals are creating fake websites that look exactly like the real thing, offering downloads of password manager software that's secretly been tampered with.

These lookalike sites often appear in search engine ads, making them hard to spot. Even for experts. Once installed, the software works normally on the surface, but behind the scenes it can steal your data or install ransomware.

Always double check the web address before downloading anything, and only get software from trusted, official sources.

TechFacts

1. Think AI is a new concept? Not really. The first computer program to have AI was Christopher Strachey's draughts (checkers) program, developed between 1951 and 1952.

2. In 2007 an estimated 10.8 trillion spam emails were sent, surpassing the 10.5 trillion legitimate messages. Spam traffic peaked in 2008, when it accounted for approximately 92% of all email traffic.

3. The term "Vaporware" was created by a Microsoft engineer when asked about the status of the company's Xenix operating system. It's often used to describe products that are announced with great fanfare but are either indefinitely delayed or never released at all.

Technology update

Full PDF translation comes to Edge

Yes, you'll be able to open a PDF in Edge, click the Translate icon, and instantly see the entire document in your chosen language. No more copying and pasting line by line.

It will support over 70 languages and be a real time saver for understanding manuals, contracts or reports written in another language.

The rollout is already happening right now.

INSPIRATIONAL QUOTE OF THE MONTH

"I have not failed. I've just found 10,000 ways that won't work."

Thomas Eddison, inventor.

Loser gets the coffees – it's time for a fun tech quiz...

1. What was the most downloaded app of 2024?
2. A blue wavy line in Microsoft Word indicates which error?
3. What does the acronym URL stand for?
4. Where are the headquarters of Microsoft located?
5. During its earliest days in development in the 1980s, what name was Windows 1.0 known by?

The answers are below.

1. TikTok with over 825.5 million downloads worldwide
2. A formatting error such as bad grammar
3. Uniform Resource Locator. It tells your browser the address to find a website or other content online
4. Redmond, Washington
5. Interface Manager

NEW TO

MICROSOFT

Pick up where you left off in Android

Microsoft's working on a new feature for Windows 11 called Cross Device Resume. It will let you pick up exactly where you left off in an app, across different devices.

For example, if you're using an app on your phone, you'll soon be able to switch to your Windows PC and carry on seamlessly, without having to start over. It's like Apple's Handoff feature and will rely on app developers enabling it. This could make switching between your devices even smoother, especially for communication, media, and productivity apps.

Your fingerprint is your password... so what happens if it gets stolen?

Biometrics are changing the way we log in.

Whether it's a fingerprint, a facial scan or even an iris pattern, more and more businesses are using this tech to access systems, files and customer records. It's fast, it's convenient. And it feels more secure than a password.

But there's a catch: If someone gets hold of your biometric data, you can't change it. You can't just "reset" your face, right?

That's why biometric data is quickly becoming one of the most valuable – and vulnerable – types of information your business holds.

And if your systems contain sensitive data about your employees or customers, using biometrics without proper protection is a bit like fitting a high-tech lock on your front door… then leaving the key under the mat.

Hackers are already targeting businesses that use biometrics for logins, because they know how powerful that data is. A stolen password can be canceled. A stolen fingerprint? That's forever.

On the dark web, biometric credentials are now being sold for high prices to criminals who know how to use them to bypass identity checks.

What can you do?

Start by making sure biometric data is stored locally on devices wherever possible, not in a central database that could become a target. If it must be stored centrally, it should be encrypted to a high level and separated from other data to limit the damage of any breach.

Access controls are also essential.

Lock down who can manage or view biometric settings and track every login attempt or change. And if you're using third-party tools or devices, choose vendors who take biometric security seriously, with strong privacy policies and a clear track record of data protection.

Biometrics can be a huge asset to your business. But with great convenience comes great responsibility. If you're going to use a fingerprint or a face as the key to your digital world, make sure you're the only one who can open the door.

Can we help you keep your biometric data secure? Get in touch.

Q: Is it really that risky to let staff use their own devices for work?

A: Yes, if it's not managed properly. Personal devices are often less secure. And if they're lost or compromised, your business data could go with them.

Q: How often should we change our passwords?

A: Actually, it's better to focus on using strong, unique randomly generated passwords with multi-factor authentication, than changing them all the time. A good password manager can help.

Q: Do we really need to back up data if we're using cloud services?

A: Yes! Most cloud services protect their systems, but not your data. Accidental deletion, user error, or cyberattacks can still result in loss.

Business gadget of the month

Ergotron LX Premium Monitor Arm

You've got a great monitor – we all know how important that is. But wouldn't it be better if it was a little higher? And maybe angled to the right?

Here's your solution: The Ergotron LX Premium Monitor Arm. Not only does it have more options to move and position your display to suit you, but it's also sturdy and pairs with almost any model of monitor.

$172.95 from Amazon.

This is how you can get in touch with us:

EMAIL: hello@digitalguidance.com
WEBSITE: www.digitalguidance.com

DIGITAL GUIDANCE