Wanted: The scams threatening your business

Introducing our 10 ‘Most Wanted’ cyber threats

Cyberattacks are a massive problem. They cost victims across the globe an eye-watering €9 trillion in 2023. And they impact businesses of all sizes.

This guide highlights the top scams to look out for, and what you need to do to protect yourself and your business against them.

brother
at your side

More than half of all cyberattacks are committed against SMEs.

60% of them go out of business within 6 months of falling victim to a hack*. A truly shocking statistic.

And even if your business survives an attack, the implications can be far reaching - from financial losses to the closure of your company.

With so many significant repercussions, we drew up a list of the most threatening cyber scams, and explored the factors that better equip businesses to deal with them.

A recent Brother survey revealed that IT decision makers feel under-equipped to deal with some very common cyber threats, with malware, ransomware and phishing attacks making the top areas that cause problems.

Maintaining secure IT systems is another universal difficulty.

44% of IT decision makers consider the management of these systems to be their biggest challenge.

So, Brother is ‘At your side’ to help.

Finding the practical information you need – what the risks are, how to spot them, and how to stay safe – isn’t easy.

So, we’ve uncovered some of the most unusual and impactful scams you should be aware of. And we’ve compiled knowledge and tools to keep you safe without slowing down your day.

Take a look at our 10 ‘Most Wanted’ list and stay one step ahead of the most menacing threats lurking on the internet.

*TechRound March 2023

Did you know?

The most impersonated brand is Microsoft (29%), followed by Google (13%) and Amazon (13%).

The scam

An employee receives a message, typically an email, from a seemingly trusted brand – Apple or Google, for example. It could even be a message on Microsoft Teams.

Like many scams, the message will say they need to take URGENT action, like divulge account, payment or password information.

Unfortunately, phishing scams usually involve impersonating well-known brands such as Microsoft, Amazon, DocuSign and Google to trick users. In fact, more than 30 million messages using Microsoft branding or mentioning Microsoft products were used in phishing attacks in 2022*.

Potential consequences for your business

By giving away even small pieces of information, hackers get the data they need to access your customers' accounts, steal passwords, and, ultimately, steal your money.

Give all your colleagues regular cyber security training, with a big focus on how to spot suspicious links. It only takes one click for disaster to strike.

Why people fall for it

This type of scam relies on the familiarity and trust we have with the brands we work with every day. That, coupled with the apparent urgency required, is why employees are taken in.

How to keep your business and colleagues safe

- Keep everyone on your team up to date with the dangers.
- Check the email address – is it the right format for the organisation?
- Does it look like a genuine email from the brand?
- Watch out for Microsoft Teams messages that look suspicious.
- Check for obvious spelling mistakes.
- Question the urgency – this is always a red flag.

*Forbes, March 2023

Just because LinkedIn is a professional social media network, doesn't make it safe.

The scam

LinkedIn is a prime target for phishing scams. Impersonators use tactics such as fake job offers, deceptive conversations about personal connections, and even potential romantic relationships. These scams, designed to trick users into revealing sensitive information, are becoming increasingly common. Once an impersonator has gained someone's trust, it's much easier to exploit them.

Potential consequences for your business

Impersonators will ask for personal data or send malware disguised as important documents, ultimately giving them access to further data, valuable files, or even business bank accounts.

Why people fall for it

This type of scam relies on the trust we have in a professional platform like LinkedIn. Fraudsters will often also impersonate recruiters, promising great benefits, and take advantage of people's wishes to work from home.

How to keep your business and colleagues safe

- Make sure everyone in your team is aware of the dangers and stays vigilant when contacted on social media.
- Be wary of unsolicited messages.
- Check any files you are asked to download.

A recent study by Check Point Research* revealed LinkedIn to be the most impersonated brand for phishing attacks

*Infosecurity Magazine, April 2022

Ask your team to be wary of any QR codes being used as multi-factor messages.

The scam

QR codes are everywhere. So, if an employee gets an email asking to scan one, they might not think twice. But not all QR codes are safe to scan.

The fake codes could pop up anywhere, but the most common places include fake multi-factor authentication or document retrieval emails, and even out in public.

A recent scam lost one woman €15,000, after she used a fake QR code to pay for parking.
The code took the 71-year-old victim to a fake website where she entered her payment details, allowing scammers to steal her payment and card information*.

Potential consequences for your business

Unsafe QR codes can redirect your employees to fake corporate websites, payment sites and malicious networks. They can secretly apply code onto their devices to ultimately steal money and sensitive data from your business.

Why people fall for it

Businesses use multi-factor authentication every day – especially when using brands like

Microsoft. People are used to supplying their details, so they often don't think twice about abiding.

How to keep your business and colleagues safe

- Keep everyone on your team up to date with the dangers.
- Think before you scan. Don't act impulsively.
- Preview the QR code link.
- Make sure the URL looks legitimate and isn't a misspelling.
- Don't scan unexpected QR codes from strangers or businesses.
- When in doubt, contact the company.

*Independent, November 2023

Giving staff access to company accounts is convenient but it comes with risks. This type of scam has cost businesses millions in the past few years.

The scam

This scam involves criminals pretending to be the bank you hold a business account with, in an effort to steal your company's money. And it's as rife in business as it is in everyday life, with an estimated half of adults receiving a phishing message like this every month.

Scammers will contact your business by phone, text, or email, often claiming a suspicious transaction needs to be verified. They'll ask you to click on a link to a spoof login page, then steal your login details to access your account. Some even use fake banking apps.

Royal haircare brand Kent Brushes know this all too well, after they lost c.€1.8m in just 20 minutes. One of their employees was tricked into giving thieves access to the company account, and the rest, as they say, is history*.

Potential consequences for your business

Once a cyber criminal has access to one account, they can hack into more, including email, bank or other financial accounts.

Why people fall for it

Businesses, like people, trust their bank. They're also wary of falling victim to fraud, so can be taken in by the 'suspicious transaction' story.

How to keep your business and colleagues safe

- Keep everyone on your team up to date with the dangers.
- Remember, your bank will never ask for passwords, or for money to be transferred to new accounts.
- Never send bank details via text message.
- Do not click on unexpected or suspicious-looking links.
- Look for spelling mistakes on bank log-in pages.

*BBC.co.uk, October 2023

No one is safe from pretexting. Even your CEO could be targeted. And the busier the person, the more likely they are to slip up.

The scam

You may have heard of a scam called ‘pretexting’. It’s where a cyber criminal impersonates a real person (usually a senior member of your company) and uses a credible narrative to trick a targeted employee. Some will even go as far as using audio clips.

They’ll ask the employee to hand over sensitive information or even money, often saying that their job depends on it.

Potential consequences for your business

These criminals do their research and use accurate information they’ve found online or elsewhere. They’ll build on this credibility with spoof phone numbers and email addresses. And it can cost your business a lot of money.

Why people fall for it

This type of scam relies on our fear of authority and losing our job. They also use real information and construct a plausible narrative.

How to keep your business and colleagues safe

- Keep everyone on your team up to date with the dangers.
- Always stop and think before taking action.
- Never send bank details via text message.
- Consider if the story makes sense.
- Contact the real person using another means of communication to verify the contents of the potential pretexting activity.

Any teams that spend money regularly (even on items like stationery) may benefit from added training on how to spot fake emails or messages.

The scam

Formally known as Business Email Compromise, or BEC, this scam involves criminals posing as potential customers before sending realistic emails to specifically targeted employees. They might request unusual payments, contain links to spoof websites, or simply ask to buy products - which will then be purchased using stolen credit cards.

Unlike standard phishing emails that are sent out to millions of people, BEC attacks are crafted for specific individuals, making them all the more difficult to detect.

Potential consequences for your business

All businesses, large and small, are at risk. 29% of firms say they have lost a client because of a BEC scam*.

MGM were victims of a BEC scam that led them to shut down their entire computer system, costing them €100m**.

Using information found on a LinkedIn post, a cyber criminal impersonated an MGM employee and called their IT department. They asked to have their password reset, and so it was. This gave the fraudster access to this employee's account and eventually led to them taking over MGM's entire system.

Everything from digital hotel room keys to slot machines stopped working, and websites for many properties went offline. Guests found themselves waiting in hour-long queues to check in and get physical room keys, or getting handwritten receipts for casino winnings as the company went into manual mode to stay as operational as possible.

Why people fall for it

Scammers will target people in your business who are likely to be spending money. They'll capitalise on the worry of costs, exploit any uncertainty in terms of revenues, and prey on businesses that are desperate for sales and payments.

How to keep your business and colleagues safe

- Keep everyone on your team up to date with the dangers.
- Stick to your official working practices relating to financial transactions.
- Be suspicious of emails from organisations you don't do business with.
- Be aware of what information is publicly available.
- Verify that people are who they claim to be.
- Use different passwords across all your accounts.
- Question any urgency.

*Security Infowatch, March 2022 **Reuters.com, October 2023

Brother printers are secure as standard, offering triple layer security at a network, device, and document level.

The scam

More than 1 in 10 security incidents that affect a business involve a printer*. It might sound like something from a cheap horror movie, but when hackers target vulnerable printing hardware, it's unnerving at best. They'll take control of your printers, and start to print out messages like 'you have been hacked,' to prove they can infiltrate your network. Then they'll threaten to take it further.

Potential consequences for your business

Beyond simply boasting about their skills, it's a way for criminals to gain a foothold in your network, so they can launch more sophisticated attacks. Printers are a way into more important resources, like file servers and email servers.

Why people fall for it

Businesses see printers as low risk. But nothing could be further from the truth. They transfer sensitive data and hackers see them as an unattended back door to your organisation.

How to keep your business and colleagues safe

- Keep everyone on your team up to date with the dangers.
- Keep your printers away from unauthorised users.
- Ask for authentication for printer interfaces.
- Use strong passwords.
- Require encryption in transit to protect printers from interception and tampering.
- Keep firmware updated.

With a secure print setup, no one should be able to gain access to your devices. Make sure that your firmware is up to date, and that all your printers are secure.

*Quocirca, October 2023

From installing anti-virus software to making sure your business's WiFi is secure, it's really important to keep your data safe.

The scam

This is probably the highest profile scam in our 'Most Wanted' list. Criminals target large organisations, often in the healthcare, financial, and energy sectors, stealing large amounts of sensitive personal data, which they then 'hold to ransom'.

They use phishing emails, stolen identities, and system security weaknesses to find their way in.

Royal Mail was hit by a ransomware attack by a criminal group, which threatened to publish the stolen information online and left Royal Mail unable to send parcels or letters abroad*.

Potential consequences for your business

In most countries, organisations are legally bound to protect any personal data they hold. And with data breaches potentially incurring significant fines, it can be very costly to your business. Currently, the average cost of a data breach is c.€5.1m**.

One of the most serious data breaches of recent times happened in the UK, when criminals targeted the Electoral Commission and got access to around 40 million people's personal information. There's no evidence to show this was exploited, but the fact access was gained is enough to prove the Commission's security wasn't strong enough***.

Why people fall for it

Criminals prey on organisational weaknesses. Compromised emails, cloud misconfiguration, unpatched vulnerabilities, and a lack of proper training are all ways in.

How to keep your business and colleagues safe

- Keep everyone on your team up to date with the dangers.
- Build security into every stage of software development and deployment and test it regularly.
- Use data security and compliance technologies that protect data as it moves across databases, applications, and services.
- Have a fully trained team ready to respond to any incident and reduce its impact.
- Implement strong data security practices and training.

Every day there are new reports of data breaches for some of the world's biggest companies. No one is immune. And they often lead to hefty fines or even prosecution.

*The Guardian, January 2023 **IBM, January 2023 ***bbc.co.uk, August 2023

**It might be tempting to snoop on unexpected scanned documents - but don't be reeled in.
(And mind your business!)**

The scam

A random email from an office printer says a colleague has received a new scanned document. All the details seem genuine. There's even a message that the document was securely scanned and a copyright notice. Then two links give them the option to view or download the document. This is actually a phishing email.

Potential consequences for your business

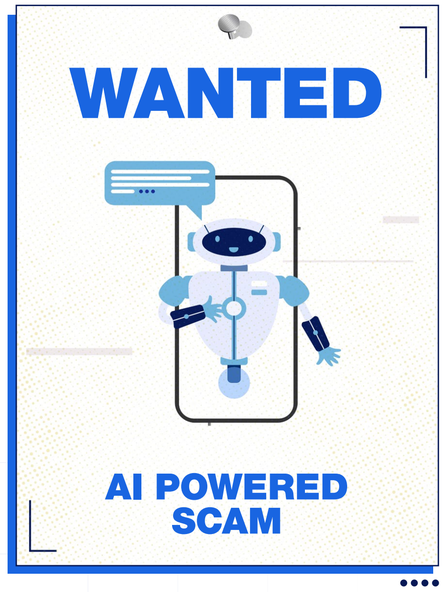
The links will take you to a fake website where scammers will attempt to extract email passwords, allowing them to send spam emails, spread malware, and potentially access financial details.

Why people fall for it

This scam is dangerous because it comes from a trusted piece of office equipment. It's also one that would rarely send you an email; this curiosity can coax you into sharing information.

How to keep your business and colleagues safe

- Keep everyone on your team up to date with the dangers.
- Be wary of attachments and links in unexpected emails.
- Only download files from trusted sources.
- Question any urgency.



AI tools like ChatGPT are making phishing emails harder to spot. This is heightening the risk to businesses.

The scam

We all know how to spot a phishing email: they're full of spelling mistakes and appalling grammar, right? Well, not anymore. Criminals are now using AI like ChatGPT and chatbots to phish with perfect grammar.

Potential consequences for your business

The result is fraudulent communications that sound more authentic, more authoritative and more trustworthy. Once trust has been gained, criminals will garner additional personal details to then impersonate known individuals or access their accounts. There's already been a 1265% increase in phishing emails – and AI has had a big part to play*.

Why people fall for it

More credible phishing emails make victims more likely to trust them and share personal and account details.

*CNBC, November 2023

How to keep your business and colleagues safe

- Keep everyone on your team up to date with the dangers.
- Be careful what information employees share.
- Don't give out log-in details and passwords.
- Be careful about publicly available data. Attackers may use it against you.
- Verify that people are who they claim to be.

Keep your business protected against the 10 ‘Most Wanted’ Scams.

Now you’ve read this guide, you know how to spot the behaviour, tactics and tricks of cyber criminals.

But, given that 60% of small businesses go out of business 6 months after a cyberattack, it’s critical that you keep referring back to this guide. Keep it handy and share it with your colleagues.

With Brother ‘At your side’, you can get ahead of the scams and look forward to a more secure future for your business.

brother
at your side