CYBER RESILIENCE

Five cyber scams to avoid now

Cyber attacks are on the rise. Knowing how to spot the warning signs makes it easier to avoid becoming a victim

Chris Stokel-Walker

To succeed in business, it has been said, you need sharp elbows and a hard head. But as well as the need to fend off competitors, vigilance for cyber attacks – and knowing how to sidestep them – is now high on the agenda of all business leaders.

Cybercriminals might be quick to devise new and increasingly sophisticated scams, hacks and fraud schemes but there are recognisable patterns. Experts reveal the top five most common types of cyber attacks to look out for.

1 Phishing

Phishing is an email or a text message spoofing an organisation or person. The aim is to trick the would-be victim into clicking on a link and entering their bank details. HMRC is commonly used in phishing attempts for organisations, while for individuals, holiday companies are the bait.

"All organisations need to deal with the threat of phishing because it's used in most cyber attacks," says Jessica Barker, co-founder and co-CEO of Cygenta, a cybersecurity consultancy. "Since technical defences have improved, cybercriminals have realised that attacks on organisations are easier, faster, cheaper, less risky and more likely to succeed when they include phishing."

Action Fraud highlights and tracks cybercrime in England, Wales and Northern Ireland. It recently highlighted an increase in phishing attacks on individuals by criminals pretending to be holiday companies with too good to be true offers. "Whenever demand for holidays soars, so does the number of scams," observes Pauline Smith, head of Action Fraud.

2 Business email compromise (BEC)

Phishing is a fundamental but small part of a set of fraud-launching platforms that target businesses. "The biggest business crime is BEC, business email compromise," says Alan Woodward, professor of cybersecurity at the University of Surrey. "It's the move from simple phishing through spear phishing to whaling, which draws in C-suite levels."

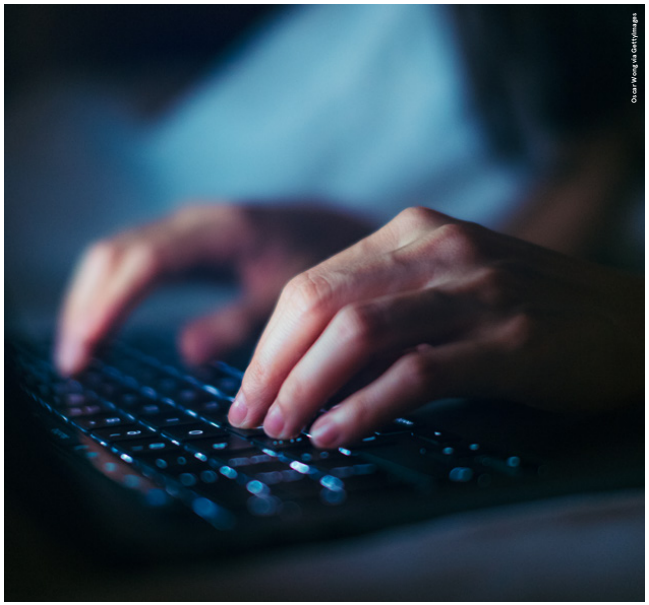
Spear phishing is a targeted version of phishing: hackers select a company or individual to attack. Whaling is a step further than spear phishing. The target here is the individual believed to hold the keys to the kingdom of the company's secrets.

A successful BEC tends to stem from social engineering or convincing someone that a hacker is whom they claim to be. Businesses need to give digital literacy training to staff at all levels. For Woodward, that means understanding the likelihood of being targeted and the ability to recognise suspicious emails. That could include checking whether the URLs in emails or text messages match the official websites. Or, if the payroll department emails a request for the company's bank account password, confirming the request offline by picking up the phone and speaking to the alleged sender. It could make all the difference between avoiding the worst or falling foul of a hack.

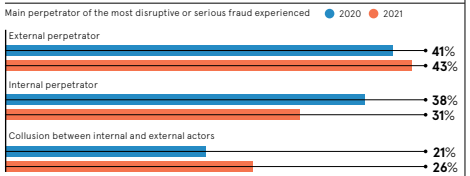
3 Ransomware

"Ransomware is the crime most organisations need to prepare for and is the most difficult to recover from," warns Woodward. "Businesses have to assume it's a case of when – not if – it'll happen and have a business continuity plan that allows the business to continue to operate and to reinstate a trusted version of the systems and network."

Ransomware isn't new, but it is increasingly sophisticated as cybercriminals change their methods to infiltrate networks and databases. "Ransomware has evolved," says Barker. "In many cases, cybercriminals don't just encrypt their victims' data. They also threaten to publicly leak it if the ransom isn't paid."


Oscar Wong via Getty Images

WHERE THE THREATS ARE COMING FROM



PwC, 2022

The potential lucre that criminals can gain from ransomware is so great that it has spawned its own mini-economy. Ransomware as a service is a niche but growing area in which criminals sell ransomware 'packages' on the dark web. This allows other criminals to launch ransomware attacks without needing any technical skill. It also means businesses can be bombarded with ransomware attempts, sent through email attachments and getting people to click on compromised websites that secretly download a virus that locks all files.

Prevention is the best cure, with good training to ensure people don't fall victim to such ploys. But the scale of ransomware attacks makes them almost an inevitability. That poses its own problems. "Many businesses have relied on insurers paying up the ransom, but that has two issues," explains Woodward. "Criminals' decryption tools are often terrible, and it's quicker to rebuild – as the Irish Health Service discovered when it was attacked in May 2021. And insurers certainly won't pay out if you haven't taken reasonable measures to mitigate losses."

4 Remote access tools (RAT)

Nobody likes rats, especially in cybercrime. Remote access tools (RATs) were responsible for £57m in losses in 2021, according to Action Fraud. It's a simple scheme, but fraudulent at its core.

The scam often begins with someone calling a company, claiming to be a representative of a trusted supplier or business partner. They could also pretend to be calling from the victim's bank to investigate a suspicious transaction on the account. They'll be deliberately confusing about the trail of actions required before offering a simple solution: to do it for them if the victim gives them remote access to their computer.

Once in, the criminal siphons off vital data and often drains any bank accounts open on the victim's computer. It's a crime often used to target individuals but can offer even bigger payloads when it targets businesses. "Only install software or grant remote access to your computer if you're asked by someone you know and trust," warns detective chief inspector Craig Mullish from the City of London Police.

5 Insider threats

Some of the biggest risks are from hackers trying to access a company's IT systems. But not every attack is launched from outside a company. "Organisations must be aware that incidents and breaches often come from internal as well as external sources," cautions Barker.

And insider attacks are severely effective. "They know the information to target and if they're successful, it can shake confidence in the organisation and damage its reputation," she says. Keeping your workers happy is vital – and keeping track of them could prevent headaches down the line. ●

> Ransomware is the crime that most organisations need to prepare for and is the most difficult to recover from

Commercial feature

INSIGHT

'The rise in the cost of living is giving criminals opportunities to scam those in need'

As cases of fraud continue to rise, chief executive of fraud prevention not-for-profit Cifas, **Mike Haley**, explores what is driving this

Q What are the Cifas databases?

A Cifas's fraud databases are the largest and most comprehensive sources of fraud risk data in the UK. Hundreds of thousands of records are added each year by Cifas members, and this data and intelligence are shared online in real time.

Our National Fraud Database holds records of fraud risk such as account takeover, identity fraud, false insurance claims, false applications and more, and organisations who use it prevent over £1bn in fraud losses every year.

Q What are some of the biggest fraud trends we are seeing this year and what is driving them?

A Instances of fraud continue to rise each year, and already we are seeing nearly 200,000 cases of high-risk fraudulent conduct recorded, up 11% on 2021.

The majority of cases relate to identity fraud, which is up a third from last year, with banking and plastic cards heavily targeted by criminals who use stolen details to apply for products and services.

Nearly a fifth of cases relate to money muling, where a person allows their account to be used, often to launder the proceeds of crime. Although most of these cases occur in the 21-30 age group, this year we're seeing a rise among 31-40 year-olds.

Recent research by Cifas showed that 17% of the public believed this type of activity was 'reasonable', so I'm concerned that people may be tempted to use this as a legitimate way to supplement their income during times of financial insecurity.

Fraud by staff against their employer is also on the rise, with cases filed to our Internal Fraud Database up by almost half from 2021. Most of these relate to individuals working in contact centres, and we know that criminals have been targeting these workers to gain access to accounts and obtain personal data.

Q To what extent is the cost-of-living crisis exacerbating already prevalent threats?

A It is providing criminals with new opportunities to scam those in need, from advanced fee fraud and obtaining loans, to investment scams attracting those looking for ways to supplement their income.

The economic crisis is also an opportunity for scammers to steal personal and financial information. Recently we've seen a rise in consumers being targeted by phishing campaigns, for example purporting to be from utility providers offering savings on energy bills or emails offering fuel vouchers, fake jobs and money-making opportunities. These emails are becoming increasingly sophisticated.

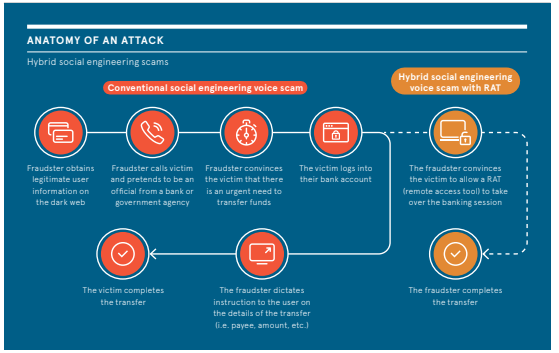
Criminals are also pretending to be from legitimate firms seeking to persuade victims to share their computer screen using remote access desktop services, and then stealing information to apply for products and services in their name or to take over their bank accounts.

But it's not just consumers being targeted. Businesses too are increasingly finding themselves under greater attack from criminals.

With an increasing number of companies looking for ways to expand their portfolio into the buy-now-pay-later space, fraudsters will look for ways to exploit any vulnerabilities within their processes.

In addition, remote working is increasing the threat of criminals paying staff to make changes to accounts or sell data. We've also seen a rise in false employment applications, with individuals failing to disclose adverse credit or gaps in their employment history, believing it will hinder their hiring opportunity. Cifas research has revealed that one in eight people believe that lying on their CV is 'reasonable', which poses a serious risk to a business and its staff. More than ever, organisations must ensure they perform rigorous checks through the employee lifecycle to identify fraud risks. ●


Mike Haley
CEO, Cifas



Outsmarting the scammers

Behavioural biometric technology can prevent fraudulent scams by detecting even the subtlest behavioural changes

Financial scams are evolving on a continual basis and becoming ever more sophisticated, making it even harder for banks and consumers to keep up.

What started as hacking accounts to steal passwords has evolved into what's commonly known as social engineering. Technically referred to as authorised push payment (APP) fraud, it involves the scammer using personal information to gain the victim's trust and psychologically manipulating them to then secure banking credentials or transfer funds to them.

In the first half of 2021, criminals stole a total of £753.9m through fraud in the UK, a 30% increase year on year, according to UK Finance, as cases of APP fraud saw a sharp increase. These scams have become so elaborate that criminals can easily circumvent one-time password authentications via SMS.

There are a host of different attack vectors too. These include phishing, where the target is asked to click on a link that then uses malware to steal the data. Vishing attacks involve an impersonator calling up and requesting updates or personal information, while smishing uses SMS to infect a device with malware, or encourage the individual to share information or unwittingly give it away by going through a multi-factor authentication.

Successful social engineering attacks require a victim taking action upon request from the criminal direction. Two examples of this are malicious payee scams and malicious redirection. The first involves duping the victim to buy items that either don't exist or are never received, while malicious redirection uses a fake or forged persona to trick the victim into transferring funds into a money mule account or an account the cybercriminal controls.

As soon as the money is received it is dispersed to multiple accounts, usually abroad, and then either cashed out or transferred to cryptocurrency, making it difficult for banks to trace and recover. The advent of instant payments has only compounded the issue.

"Cybercriminals feed on people's fear and anxiety to prize sensitive information away," says Gadi Mazor, CEO of BioCatch. "The Covid-19 pandemic and cost of living crisis have acted as a hotbed for cybercrime and specifically social engineering attacks."

Stolen personal information can be used to open a fraudulent bank account, take over an existing one or to manipulate the user into transferring their own funds to the cybercriminal. The consequences of becoming a victim of these scams can be devastating, not only financially but reputationally too.

As the criminals become smarter in their techniques, businesses must stay one step ahead. While companies have introduced additional layers of security, such as longer passwords and two-factor authentication, to protect against scams, these often detract from user experience and don't provide protection against sophisticated social-engineering scams.

To overcome the new breed of fraud without impacting experience, BioCatch has established an AI-based solution that analyses behavioural insights and patterns to uncover scams. By using AI and machine learning, it analyses a range of different factors, such as how users are holding their device or the speed a password is typed in, to detect suspicious activity. During an average session it analyses more than 2,000 distinct data points.

The technology then compares the user's activity with the known individual's typical behaviours to see if they are consistent. After the data is collected, these behavioural insights can be used to inform new strategies and enable firms to respond to such threats in real time.

"The cybercriminals of today manipulate people to give away their own details and make fraudulent transactions. On the surface, this means everything will match the bank's records, making traditional fraud detection controls defunct," says Mazor.

"The one element that gives them away is the change in the user's genuine behaviour – thus giving us critical clues of financial fraud. Modern behavioural biometrics monitors and analyses these behaviours continuously and in real time to protect financial institutions and consumers before they are impacted."

> Scammers capitalised on the pandemic, which gave rise to a multitude of unusual financial transactions

For more information about BioCatch's behavioural biometric solution, visit biocatch.com

BioCatch