Secret signs

YOUR INTERNET SECURITY HAS BEEN COMPROMISED

BY JULIET MORAN, TELEPHONESYSTEMS.CLOUD

JULIET MORAN

BUSINESSES HAVE BEEN TOLD OF THE TELL-TALE SIGNS TO ASSESS WHETHER THEIR INTERNET SECURITY HAS BEEN COMPROMISED.

ONLINE CLOUD EXPERTS FROM TELEPHONESYSTEMS.CLOUD HAVE SHARED THEIR TIPS WITH BROADBAND JOURNAL. TAKE NOTE.

Businesses have been warned to look out for tell-tale signs their internet security has been compromised.

With cyber security threats a very serious problem to businesses, online cloud experts from TelephoneSystems.Cloud have shared the signs that should be monitored to ensure that there has not been any breaches.

When a business's internet security is compromised, there are some unique signs beyond those that affect individuals. These can range from operational disruptions to financial anomalies.

According to figures from The Cyber Security Breaches Survey, half of businesses (50%) experienced some form of cyber security breach or attack in the last 12 months. For medium businesses the number was 70% and for large businesses 74%.[1]

If a business suspects a breach it's crucial to take action quickly to investigate the scope of the attack.

Some of the specific business threats include unexplained data leaks, unauthorised activity from employee accounts new or unknown administrator accounts and a sudden increase in targeted phishing emails.

Businesses may also see some financial discrepancies if there has been a breach. Unauthorised fund transfers or invoices paid to unverified vendors might be the result of a business email compromise or financial malware.

Juliet Moran from TelephoneSystems.Cloud says: "It's crucial for all businesses to take digital security seriously, and knowing what the key signs to look out for are can help to tackle any problems as quickly as possible.

"Smaller businesses especially can benefit from knowing what to monitor, as they are more likely to lack the infrastructure of larger businesses that have specialist teams in place to help prevent security breaches.

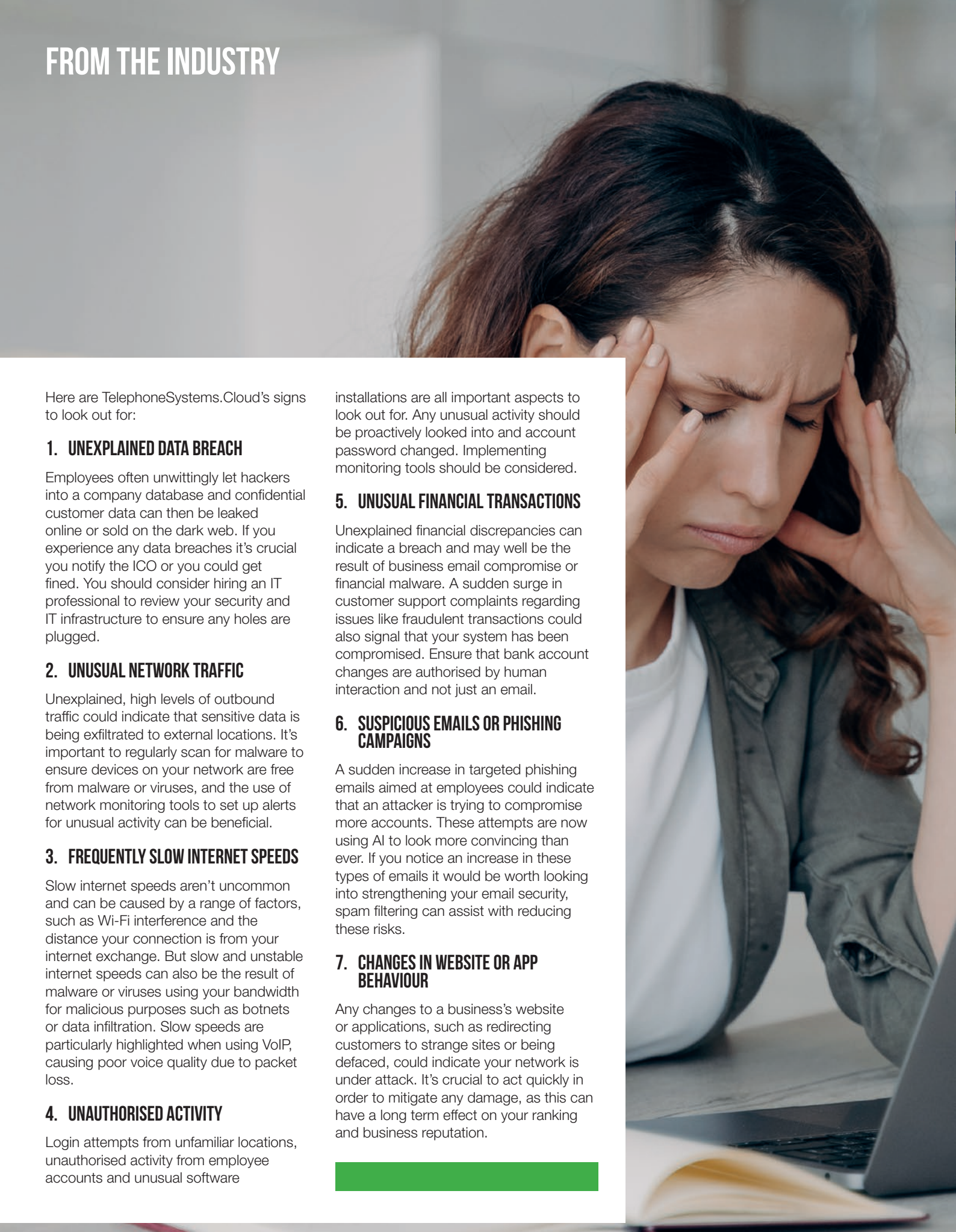
"Unexplained data leaks is a huge indicator there has been a breach to your business and probably the most obvious one, but there are many more subtle breaches that may be taking place that you should be trying to monitor.

"Unauthorised activity from employee accounts and any login attempts from unusual locations and unfamiliar IP addresses can signal unauthorised access attempts and should be monitored.

"The sudden appearance of unfamiliar administrator accounts or changes in access levels could also show that an attacker has managed to gain elevated access in your business's network.

"And any financial anomalies such as unauthorised fund transfers should be taken care of immediately in case there's any financial malware."

1 *https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024#:~:text=Half%20of%20businesses%20(50%25),in%20annual%20income%20(66%25)*



Here are TelephoneSystems.Cloud's signs to look out for:

1. UNEXPLAINED DATA BREACH

Employees often unwittingly let hackers into a company database and confidential customer data can then be leaked online or sold on the dark web. If you experience any data breaches it's crucial you notify the ICO or you could get fined. You should consider hiring an IT professional to review your security and IT infrastructure to ensure any holes are plugged.

2. UNUSUAL NETWORK TRAFFIC

Unexplained, high levels of outbound traffic could indicate that sensitive data is being exfiltrated to external locations. It's important to regularly scan for malware to ensure devices on your network are free from malware or viruses, and the use of network monitoring tools to set up alerts for unusual activity can be beneficial.

3. FREQUENTLY SLOW INTERNET SPEEDS

Slow internet speeds aren't uncommon and can be caused by a range of factors, such as Wi-Fi interference and the distance your connection is from your internet exchange. But slow and unstable internet speeds can also be the result of malware or viruses using your bandwidth for malicious purposes such as botnets or data infiltration. Slow speeds are particularly highlighted when using VoIP, causing poor voice quality due to packet loss.

4. UNAUTHORISED ACTIVITY

Login attempts from unfamiliar locations, unauthorised activity from employee accounts and unusual software installations are all important aspects to look out for. Any unusual activity should be proactively looked into and account password changed. Implementing monitoring tools should be considered.

5. UNUSUAL FINANCIAL TRANSACTIONS

Unexplained financial discrepancies can indicate a breach and may well be the result of business email compromise or financial malware. A sudden surge in customer support complaints regarding issues like fraudulent transactions could also signal that your system has been compromised. Ensure that bank account changes are authorised by human interaction and not just an email.

6. SUSPICIOUS EMAILS OR PHISHING CAMPAIGNS

A sudden increase in targeted phishing emails aimed at employees could indicate that an attacker is trying to compromise more accounts. These attempts are now using AI to look more convincing than ever. If you notice an increase in these types of emails it would be worth looking into strengthening your email security, spam filtering can assist with reducing these risks.

7. CHANGES IN WEBSITE OR APP BEHAVIOUR

Any changes to a business's website or applications, such as redirecting customers to strange sites or being defaced, could indicate your network is under attack. It's crucial to act quickly in order to mitigate any damage, as this can have a long term effect on your ranking and business reputation.