Mobile Banking App is HERE!

UNION BANK

January 2024

Phishing, BEC, and Check Fraud: The Top Fraud Trends in 2023

These are the top cybersecurity and fraud trends that affected businesses in 2023.

Threat actors have been busy this year turning inboxes and mailboxes into fraud minefields. While phishing scams and check fraud have been around for years, the sharp rise in these fraud attempts highlights the need for organizations to remain vigilant and consider strengthening defenses to protect themselves against costly breaches.

Fraudsters are still going phishing to snare victims

Phishing is a form of social engineering used to harvest sensitive information, from which they can determine how to further exploit the victims. Cybercriminals exploit our inherent helpfulness and trustworthiness through these types of fraud attempts, which is why they're so successful.

Most people are aware of phishing scams – we've heard about them on the news, social media, and cybersecurity training. Despite this awareness, a 2022 Verizon report found that 82% of reported breaches involve the human element. Additionally, though the report found that just 2.9% of phishing emails were clicked on, these breaches could lead to more than 33 million accounts being compromised.

The financial consequence of a successful data breach is another reason phishing can be so dangerous. Data breaches resulting from successful phishing attempts averaged $4.91 million globally in 2022, making it one of the most expensive forms of fraud.

Think before you click to help avoid phishing scams:

- Never click links or open attachments from unknown senders or suspicious emails.
- Hover over URLs in emails to check the link before clicking on it.
- Don't assume a branded email is safe – fraudsters can mimic logos.
- Watch out for urgent, demanding, or threatening requests.
- Check for brand indicators for message identification (BIMI), which indicate an

Continued on Page 2

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
740-374-0010
By Appointment Only

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

email is validated and trusted.

- Develop a robust data recovery and protection plan to minimize the damage of a breach.

Business email compromise is costing companies big money

There's a reason why the FBI says business email compromise (BEC) was one of the costliest forms of cyberattacks.

BEC is a form of phishing that targets employees by impersonating vendors or leadership members and requesting employees take some financial action. Victims of BEC might find themselves on the receiving end of a seemingly innocent email from a vendor asking them to update bank account information or submit an invoice to a new entity. The fraudster might have compromised the vendor's email account or, more likely, have made minor, easy-to-miss adjustments to the known email address.

Often, because the business originated the payment, these funds result in a loss that can only sometimes be recovered. When compromised, an organization's best chance to remedy a potentially devastating situation is to act fast.

Employee training and an incident response and data recovery plan can increase your chances of catching a BEC attempt before it's too late.

Verify requests and act fast to help protect against BEC:

- Call vendor contacts or people within your organization at a known or confirmed number to verify any request to change invoicing or financial information, send payments to an unknown destination, or purchase gift cards.
- Be suspicious of changes in business practice, such as a known contact requesting you email them via a personal email address.
- Avoid responding quickly when an email requests you take urgent action.
- If you are a victim of business email compromise, immediately contact your bank and submit a claim to the FBI's Internet Crime Complaint Center.

Check fraud is on the rise – again

What's old is new again as we look ahead to 2024. Despite predictions just a few years ago that check use would dwindle into nonexistence, individuals, businesses, and government entities continue to rely on checks. Cybercriminals have taken advantage of this fact in recent years, as evidenced by check fraud doubling in 2022. The financial ramifications of check fraud can be overwhelming: Check fraud lead to $24 billion in damages in 2023.

Much like phishing scammers, bad actors committing check fraud rarely work alone. A black market has even emerged for stolen checks.

While banks are required to return fraudulent funds in the case of check fraud, there is no set timeline for them to do so. Claims can drag on, leading customers to be without their funds for months.

Stay one step ahead of check fraudsters:

- Leverage electronic payments whenever possible.
- Consider sending checks through UPS-certified mail or another tracked mail system.
- Bring checks to a post office instead of putting them in an outgoing mailbox.
- Depending on your bank, use available security measures to review checks and approve or decline them to help catch fraud early.
- Separate employee fiduciary duties within your organization, so the person writing the checks isn't also responsible for cashing them and reconciling accounts.

Keep cybersecurity & fraud prevention top of mind in 2024

The threat landscape is ever evolving, and how organizations can best protect themselves is constantly shifting. Despite the specific threats looming on the horizon, it is essential to remember that an overall cybersecurity and fraud prevention strategy should be a priority for organizations of every size.

Sources/Credit:
Article:
Huntington
Images:
Image by Pete Linforth from Pixabay,
Image by Cliff Hang from Pixabay,
Attribution: Pixabay, Pixabay Content License Summary

Robocalls Keep Coming Despite Efforts to Crack Down. Here's How to Protect Yourself

Our phones keep ringing with unwanted robocalls. Washington said it was getting tough.

So, what happened? Will those calls ever stop?

When the phone rings

When spammers call and call and call, apps like Robokiller block them.

A month-by-month chart from Robokiller shows a robocall rollercoaster. Tall peaks and deep valleys repeat.

This past summer, robocalls dipped from a high of almost 8 billion a month. It turns out, the Federal Communications Commission took legal action targeting some companies that make bulk robocalls.

The FCC says its steps resulted in an “88% month-to-month drop in student loan scam robocalls,” plus a “99% drop in auto warranty scam robocalls.”

And yet, our phones keep ringing. It’s like Whack-A-Mole. The crooks keep finding ways to circumvent the protections the FCC put up.

For example, Robokiller says robocalls shot back up to about 6 billion in March – just a few months after the FCC’s victory lap.

So, what can you do?

Consumers can install a robocall blocker – for a fee. Robokiller is just one of many.

You can get a free 7-day trial to test it out and see if it makes a difference for you.

Or, you can check with your phone carrier. See if it offers a free blocker like T-Mobile’s “Scam Shield.” It identifies if a call is most likely to be a scam, and it’s 99% accurate.

T-Mobile says it’s intercepting tons of spam calls. More than 40 billion spam calls on the T-Mobile network were blocked in 2022 alone.

If an unknown call gets through, practice self-restraint. If you don’t recognize a number, don’t pick up. If you do pick up, and it’s not somebody you know, and you’re certain it’s not somebody you know, just hang up.

Sources/Credit:
Articles:
NBC Bay Area
Image:
Image by Jan Vašek from Pixabay; Image by Gerd Altmann from Pixabay; Attribution: Pixabay, Pixabay Content License Summary