Mobile Banking App is HERE!

UNION BANK

January 2023

Cybercrime Outlook 2023: It's All About the Economy

Member FDIC

Who likes inflation, rising interest rates, layoffs and soaring gas and food prices? Cybercriminals. And because these struggles will likely continue impacting the economy in 2023, these online scammers should be happy, and wealthier, next year as they con unsuspecting people seeking financial relief.

Economic challenges cause many to change their daily behavior. Some will seek financial assistance from the government. Others will try to land side hustles to pad their bank accounts, while still others will be desperate enough to hope that surprise lottery "winnings" are real.

This creates the perfect environment for scammers, who can use texts, emails, and phone calls to trick desperate victims into surrendering their personal information, emptying their bank accounts, or spending big dollars for services or lottery winnings that never come.

It's the economy, then, that will have the greatest impact on the spread of cybercrime in 2023. Here are our predictions for why.

1. Economic trouble could lead to more scammers trying to earn money – and more victims desperate to save.

As inflation and interest rates continue to rise, consumers will struggle to keep their bank accounts full. Consumers are spending more at the pump and at the grocery store. Borrowing money to pay for cars and homes is getting more expensive thanks to soaring interest rates. These are difficult times for many.

Scammers know this. They also know that consumers are at their most vulnerable when they are worried about their financial health.

Expect a rise in several financial-based scams:

1. Assistance scams: Cybercriminals will reach out to consumers by text, phone, or email to inform them of fake government assistance programs. These messages might claim that consumers can qualify for reduced electric or heating bills or that they are eligible for low-cost government meals and utility subsidies. All the recipients of these messages must do is click on a link, send a small payment, or make a phone call.

This is all a scam, though. Consumers might click on a link that takes them to an online form. To qualify for government assistance, victims must provide personal information such as their name, birthdate, address

Continued on Page 2

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
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

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

and Social Security number on the form. When they click "Submit," though, their Personal Identifiable Information – or PII -- is sent to a criminal.

That criminal can then use this information to take out loans or credit cards in the victim's names. They might use it to access their online bank and credit card accounts. They might sell the information on the Dark Web to the highest bidder.

2. Shopping deals: Scammers will send victims messages promoting low-cost clothing, electronics or groceries. They'll set up fake e-shops promoting brand-name items at bargain prices. Again, though, these deals are a scam. The fraudsters behind them will try to steal victims' personal information or convince them to send online payments for bargain products that aren't real. Once consumers send their payments? The entrepreneurs behind these deals and e-shops disappear.

3. A bit of romance? When the economy suffers, people may also be impacted emotionally. Whether they are struggling from recently losing their job or overall despair from financial instability, some might also be suffering from a bout of low self-esteem. This makes them especially vulnerable to online romance scams.

In these scams, criminals strike up a relationship with victims online, sending emails, communicating in chat rooms and buzzing their victims' phones with amorous texts. After building up trust, the scammers, after promising to soon meet their victims in person, ask for money or ask for you to help move money around.

As scammers and consumers get more desperate to pay their bills, we expect to see an increase in scams, and an increase in people falling victim to those scams. So stay alert as you navigate online.

2. Companies trying to cut costs could lead to more breaches caused by chaos and sabotage, which can trickle down to making consumers vulnerable.

The economy's troubles will impact companies in 2023 as well. We have already seen many technology companies reducing and reorganizing staff, and it is likely to continue into next year. And when companies are operating with smaller staff and the people are taking on new responsibilities, you can expect that some companies will become more vulnerable to data breaches, ransomware attacks, and other cybercrimes, because of the changes.

3. With more advanced and open generative AI frameworks available, more scammers could start to use these technologies in high-touch interactions such as romance scams.

Last year, we predicted that criminals would take advantage of improving AI technology to boost the effectiveness of their scams. That prediction turned out to be accurate. And next year? Expect scammers to continue to wield AI in their crimes as this technology becomes even more accessible and easier to use.

Programs such as Dall-E, Midjourney, and Stable Diffusion allow users to create images by describing a picture. These models will create several versions of the images that users describe. This technology can be a powerful tool when wielded by cybercriminals.

Con artists can use these AI tools to create images of the person they are pretending to be and even place them near specific geographic landmarks to add some veracity to their fake personas. It's a way to add more depth to an old scam and to more easily persuade a victim to send cash or provide their credit card information.

4. Weaker versions of 2FA could be exploited, leading to breaches in companies, which can lead to more consumer information exposure.

Criminals are devising attacks meant to breach standard multi-factor authentication technology. Despite this, we still don't see many companies adopting stronger two-factor authentication (2FA) practices for either customers or employees in 2023, which can impact consumers.

That's a problem. Companies that continue to use weak 2FA are inviting cybercriminals to steal important credentials. That leads to serious data breaches and cybercrimes.

The key is for companies to turn to what are known as unphishable factors when setting up their 2FA systems. Unphishable factors are those that criminals can't trick employees into providing. They include such factors as biometrics, device-level security checks, hardware security keys, and cryptographic security keys. Over time, companies will start to deploy these more secure authentication technologies, but it won't happen anytime soon.

Unfortunately, too many companies rely on phishable factors, those that are easier for criminals to intercept. These phishable factors include passwords, security questions, SMS text messages, and time-based one-time passwords. All of these can be intercepted and used to authenticate.

Consumers can help protect themselves from these types of threats. Make sure your password is unique and avoid using the same one across different accounts.

The Final Word

Challenging economic times make people desperate, often desperate enough to fall for different types of scams. Stay alert this year while living your digital life, because scammers are always finding new ways to trick unsuspecting victims—especially when they are most vulnerable. Remember, if something seems too good to be true online, it probably is.

Source: ***Norton Labs , December 1, 2022***

5 Scams To Watch for in 2023

As cybercriminals find new paths to ill-gotten gains, here are the types of scams we can expect to see in the coming months.

1. Business Email Attacks

Business email compromise (BEC) attacks lead this list, as these scams can have attractive payouts. BEC-related losses totaled nearly $2.4 billion in 2021, according to the most recent report from the FBI's Internet Crime Complaint Center.

These scams involve spoofed emails that look like they're coming from a trusted source such as a company executive, employee or vendor. They typically ask the recipient to transfer funds urgently and rely on manipulative social engineering tactics to get their victims to act quickly.

One common attack is the payroll diversion scam. Scammers masquerading as an employee will email the payroll team to change their direct deposit account details. Sometimes the emails are obviously fake, filled with grammatical errors and sent five or six times a day to the same payroll employee.

Other times, the emails look legitimate and contain a good backstory to lend credibility. A year ago, fraudsters typically would impersonate company executives, presumably because their paychecks would be larger. Recently, we have observed a shift in tactics, with mid-level employees being impersonated more often.

2. Malware and Ransomware Threats

These incidents tend to garner a lot of media attention, like the Colonial Pipeline ransomware attack in 2021. It temporarily took out a major fuel supply system in the southeastern U.S. and resulted in a $4.4 million payday for the hackers.

We'll likely see more of this type of activity, particularly related to the conflict in Ukraine and the associated sanctions. Russian state-sponsored organized crime teams that excel at ransomware will help sustain the war efforts.

U.S. government agencies, defense contractors and other organizations assisting with Ukraine's defense will be targeted with phishing emails aimed at creating havoc.

3. Crypto Scams and 'Pig Butchering'

Using translation programs to communicate with global victims, scammers looking for a payout launch what authorities call "pig butchering" scams.

They'll message someone's phone, dating app or WhatsApp with a "Hey, are we still on for lunch Friday?" The goal is to see if they can get a response and then build an online friendship.

Eventually, they'll ask if the victim knows anything about crypto to lure them onto a sham website where the fraudsters say a friend made a lot of money.

If the victim invests, they'll see rapid returns that lure them into pouring in more money. The scammers are basically "fattening the pig" until it's time to butcher it—when they take all the money out of the account.

4. Innovation in the Cybercrime Cash-Out Process

The place where threat actors are most likely to get caught is in the cash-out. The reason is that law enforcement can start following suspicious activity more easily once transfers surpass $10,000 for standard bank accounts.

Cryptocurrency has been somewhat easier for authorities to track, which is leading to a rise in crypto mixing services. These evade scrutiny by taking in traceable "dirty" crypto and cleaning it so it can't be traced back to a ransomware attack or other cybercrime.

Gift cards present the lowest-risk cash-out for cybercriminals because there's little to no traceability. However, potential targets are smartening up and realizing that "the IRS" isn't going to ask for a payment using gift cards—or crypto, for that matter.

Given these dynamics, we'll likely see criminals seeking new ways to launder their illegal proceeds in the shadows.

5. Cybercrime and Scamming as a Service

Just like the rest of us, fraudsters like a good one-stop shop. Underground virtual marketplaces are springing up with end-to-end services that enable low-skill threat actors to fill their carts and pay with crypto.

They can procure sets of stolen credentials, credit card numbers, phone numbers, phishing kits, ready-to-roll malware and other tools to carry out bank fraud, ransomware attacks, phishing campaigns and more. We'll see an increase in these types of services in 2023.

Looking Ahead

Yes, scammers are inventive. Yes, they will continue to try and steal our money in dozens of resourceful ways.

But we're all becoming more educated cybercitizens, increasingly able to spot and fend off malicious campaigns.

Source: *Forbes, John Wilson, Contributor, December 19, 2022*