PHISHING SCAMS:

BBB study tallies record number of reports as scammers adopt new technologies

BBB

ISSUED: JUNE 2024

INTRODUCTION

Are you thinking about clicking on an unknown link in your email? Think again. Since early 2021, the Better Business Bureau® (BBB®) received more than 23,000 reports related to phishing, which is a scam tactic that fraudsters use to trick consumers and employees into revealing personal information about themselves or the companies they work for.

Reports totaled over 9,000 in 2023, more than double the previous year and a record high. With the current year's reports trending toward another record, phishing is clearly on the rise. Cybersecurity experts say artificial intelligence and text-based scams have contributed to that spike. And consumers aren't the only group at risk. Businesses lose millions each year in sophisticated phishing scams that prey on weaknesses in companies' cybersecurity policies and training.

Every scam starts with a fraudster attempting to reach out to their target, and they use any means possible, whether by phone, text, voicemail, email or even a letter in the mail. The more sophisticated ones may even set traps for you, planting them on the web and inside search engines, waiting to reel you in. Regardless of the method of communication, when a scammer tricks a person into clicking a link or visiting a malicious website, it falls under one category: phishing.

Phishing dates back to the '90s. This BBB study will lay out some of the most common ways it has adapted and grown since then. BBB interviewed dozens of scam survivors, experts and regulators. Taken together, their insights reveal a growing sophistication in phishing, making it one of the most complex and varied scams out there.

CYBERSECURITY EXPERTS SAY TEXT-BASED FRAUD AND ARTIFICIAL INTELLIGENCE CONTRIBUTED TO RECORD NUMBER OF REPORTS IN 2023.

ABOUT THIS STUDY

We are focusing on patterns of reports from the public about scams they have encountered. Through an analysis of the reports, BBB studies are intended to give consumers, businesses, news media, researchers and regulatory agencies an in-depth understanding of:

- **How these scams work**
- **How to avoid common scams**
- **What type of enforcement is helping curb fraud**
- **Red flags for consumers and businesses**

CONTENTS

PHISHING SCAMS

A LONG-LASTING BUT EVER-EVOLVING FRAUD

Nearly every internet user has received a junk email impersonating a well-known company. Embedded within those emails are links: These are phishing attempts.

Take **John** in Bridgeport, Connecticut, for example: For months, he has received hundreds of emails from a scammer pretending to be from Geek Squad, Best Buy's computer repair service. While the contents of the message changed, each one attempted to steal personal information from him.

Phishing scams often focus on stealing sensitive information like bank account numbers, login information, passwords or credit card numbers. They hope to use this information to access other accounts and eventually steal cash.

"I contacted Google about the issue to explain how I am trying to deal with the volume of messages from this address," John told BBB. ***"I receive 20-50 emails a day from this address. Most go to spam, but they still require review and deletion."***

More than 250 reports to BBB Scam Tracker℠ involved Geek Squad impersonations, many of which employed tactics used in tech support scams.

Phishing takes many forms, but at its core, it is a cybercrime in which scammers attempt to contact their target to get them to hand over sensitive information. The deception often comes in the form of a malicious URL or a shared Word Document that tasks the person to share information, sometimes without them even realizing it. The scam originated in emails,

but has broadened to include SMS text messages, phone calls and even QR codes to steal personal information, passwords and eventually money.

Some scammers may impersonate well-known websites like banks or social media to steal information. And other times, their phishing attacks are attempts to install malware onto the user's device, allowing fraudsters to seize control of it.

Phishing attacks are orchestrated broadly by fraudsters and even foreign state-run groups throughout the world, making it hard to track down the source without significant investment and resources. The ubiquity of the scam, though, means it is an international threat to anyone using the internet.

Monetary losses are severe, as reports to the Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) totaled over $18.7 million in stolen funds in 2023.

BBB SCAM TRACKER PHISHING REPORTS

Source: BBB Scam Tracker (2021-2024, Q1)

YEAR	REPORTS	MEDIAN LOSS
2021	5,374	$300
2022	5,101	$300
2023	9,288	$313
2024 (Q1)	3,363	$317
Total/Average	**23,126**	**$300**

PHISHING SCAMS

Most of the time, email service providers send phishing messages directly to a spam folder or they are marked as suspicious. But when the email appears to come from a trusted party, it can be difficult to resist the urge to share personal information.

Paul told BBB he received an email from Meta's advertising department. The message claimed a Facebook page he ran had inappropriate content and provided a link to review. Paul clicked and signed in, unknowingly sharing his login information.

Once he did, the scammers posted illegal content on his website, saying he was at risk of breaking the law. Paul knew something was wrong at this point as he had never posted any of the things he was accused of, and he cut off contact. ***"I turned it off as soon as I saw what it was and called the police and the FBI,"*** he told BBB.

When a fraudulent message steals the likeness of a business you frequent – a social media site, the utility company or even the government – it doesn't take much for scammers to get exactly what they came for: personal information and cash.

Even if a scammer doesn't steal money right away, the Federal Trade Commission says they can often enter linked accounts, compile enough personal information to break into more sensitive logins like banks, and even financially extort the person for cash.

Bob in Atlanta, Georgia dealt with an impersonation of a company he knew well. He told BBB he received an email claiming to be from PayPal. It said he needed to confirm his account and provided an attached document, a common tactic used to replace links in phishing scams. When Bob opened the document, he saw a space for him to enter the last four digits of his Social Security number. This set off alarm bells for Bob, and he declined, avoiding a serious breach of security information.

Sometimes scam survivors can escape with minimal losses, but the most convincing fraudsters can take substantial funds before being detected.

Patti in White Bluff, Arkansas told BBB in March 2024 that she received a call from someone claiming to be with the FBI. The agent said the investment company Patti used for retirement was fraudulent and to protect her funds, she needed to transfer them into an FBI holding account. Patti liquidated $300,000 and sent it.

It took Patti weeks to tell anyone about her experience, until the financial pressure of the lost money became too large.

Phishing grows more complicated with each passing day, even though the root of the scam dates to the early days of the internet in the mid-1990s.

Consumers using AOL, then known as America Online, were sent a fraudulent link in their emails, according to The Washington Post. Once clicked, they were prompted to "enter their name and address as well as their home phone and credit card numbers to update AOL's new computers."

Now, these types of email phishing scams seem easy to spot. But a feeling of confidence can fade quickly when a scammer uses more sophisticated methods.

Lydia in Orlando, Florida experienced firsthand how convincing scammers can be.

"When my Frontier Airlines flight was cancelled due to weather, I did a (internet) search for Frontier Airlines customer service," Lydia told BBB in April 2024. ***"I found a link, called the number and the person proceeded to tell me Frontier's policy for cancelled flights."***

Lydia didn't realize that scammers can plant links like the one she clicked, and everything sounded reasonable when they said she needed to pay the $125 difference between her cancelled flight and the next available one. It wasn't until she examined an official-looking confirmation email, which had an unrelated domain name, that Lydia realized she had been scammed.

PHISHING SCAMS

BBB Tip: Double check any phone number found through a web search.

While bait planted for Lydia was left out in the open, this type of scam still falls under the phishing umbrella. Called search engine phishing or SEO poisoning, according to security experts, this newer and more complicated phishing scam subcategory preys on a target's familiarity with search engines to get them to do what all other phishing attempts do: click on a malicious link and share personal information or download malware.

The longevity of this scam shows not only its effectiveness, but also gives a timeframe to examine how it has developed alongside evolving technology.

"As far as what I am seeing, every cybercrime seems to begin with a phish," said Timothy Gallagher, a former FBI cybersecurity expert and Chief Security Officer of Nardello & Co. ***"Phishing is really part of everything."***

BBB SCAM TRACKER PHISHING REPORTS BY TYPE

Source: BBB Scam Tracker (2021-2024, Q1)

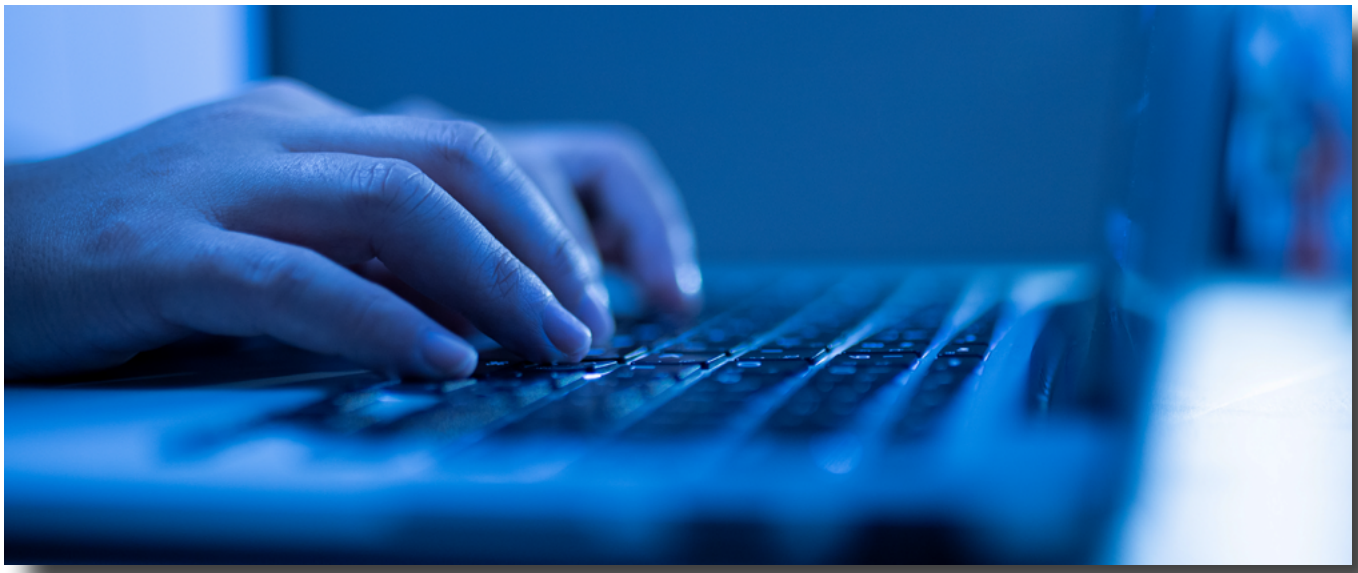
SCAM TYPE	REPORTS	MEDIAN LOSS
Phishing	9,793	$249
Vishing	9,031	$500
Smishing	3,744	$200
Pharming	348	$599

PHISHING MEETS GENERATIVE ARTIFICAL INTELLIGENCE

Simple phishing done through email might seem like an old school scam, but fraudsters are always coming up with novel ways to ensnare the public. Spear phishing or whale phishing, a process where scammers target specific individuals with phishing attacks, is common, but the most commonly encountered attacks are the result of fraudsters casting wide nets meant to trap thousands of random people in their phishing schemes. To do so, they reach out to as many targets as possible, taking advantage of whatever methods they can to increase the speed and volume of fraud messages sent out. Scammers have found success with both methods.

Recently, scammers appeared to have leveraged artificial intelligence (AI) to increase their reach. WormGPT, first reported on by SlashNext, is a publicly available generative AI and cybercrime tool. Generative AI is a tool that can help users create new text, images, videos, music and other types of media from a simple prompt created by the user. Over the last year, the use of AI chatbots to craft messages has exploded in popularity.

Widely used chatbots are created with ethical guidelines meant to prevent the AI from putting out answers which could harm others. The creators of WormGPT removed those ethical guidelines, allowing scammers to craft more convincing scam messages than ever. The introduction of widely available AI took off in 2023, coinciding with the rise in phishing reports to BBB Scam Tracker. SlashNext itself also noted a nearly 1,300% increase in phishing attacks from the end of 2022.



The group said in their report that the launch of generative AI ***"is not a coincidence in the exponential growth of malicious phishing emails as the use of chatbots contributed to the increase as more cybercriminals were able to launch sophisticated attacks quickly."***

Gallagher said the influence of AI is clear. ***"When you look at emails and you see the grammar, you aren't seeing the stilted language anymore."***

And it isn't just the ability to write messages faster and clearer. Gallagher said the ability to leverage AI and machine learning to study weaknesses in systems gives scammers a way to refine their tactics in a novel way.

"They maybe send an email repeatedly, and they use machine learning to see what they need to get it through," he said. ***"The good news is that the good guys have the same tools. The issue is that threat actors play by bad-guy rules."***

BUSINESS EMAIL COMPROMISE (BEC) SCAMS

A COSTLY FRAUD FOR THOSE CAUGHT WITHIN IT

There are few frauds as costly as BEC scams. In 2023, IC3 received over 21,000 BEC complaints. Losses totaled $2.9 billion, with the average loss reported as $174,000. BEC scams operate like other phishing scams, but they target businesses instead of customers. Fraudsters know companies are much more likely to be sending large chunks of money regularly, and simply intercepting one of those wire transfers can lead to an enormous pay day.

BBB Report: How ignoring urgent threats can help avoid scams

John in Seattle, Washington told BBB his nonprofit, of which he is the president and chief executive officer, received a threatening email in April 2024. The sender claimed his organization had not trademarked its name and was at risk of forfeiting its legal right to use it within the next 24 hours. To prevent that from happening, John needed to click on a link and follow the instructions.

Instead of panicking, his organization contacted the United States Patent and Trademark Office (USPTO) and was able to confirm its trademark. John avoided the scam, and the likely monetary loss which would accompany it.

BBB Warning: Twenty different BBB Scam Tracker reports involved USPTO scams. Be wary of unexpected messages about trademark issues.

Well-trained employees can spot phishing emails quickly, and a strong chain of reporting can help stop scams in their tracks. **Stephanie** in Springfield, Missouri told BBB she received an email from the accounting department at work about an invoice. She realized she didn't recognize the email and reached out to her IT department head. They identified it as a scam and cut contact before any documents were opened.

Fraudsters impersonate many other departments, including human resources and IT. They may also opt to attack from the outside, infiltrating and posing as vendors. In early 2023, a business in St. Louis told BBB it was undergoing significant renovations. To outfit the building with furniture and other necessities, the business contacted a well-known vendor to complete an order. The two had worked together previously. The vendor visited in person to hammer out some final details and said they would send an invoice over email. Unbeknownst to both parties, the vendors' devices had been compromised by a scammer, who intercepted the invoice and sent their own wire information.

The business, having just seen the vendor, wired the requested $70,000 immediately. The next day, when someone at the business called to check in with the vendor, they said they hadn't gotten a wire and both parties knew something was wrong.

"We are a small-to-medium sized company, so that was a lot of money," an executive at the company told BBB. Knowing a scam might be involved, the company immediately called their bank, which was able to freeze some of the funds. In the end, they recovered all but about $7,000. The executive told BBB it was an expensive lesson. ***"Any time a vendor requests electronic funds, I need it in writing, and I am going to call you and have a verbal conversation,"*** they said.

BBB Tip: Set up multi-factor authentication for invoices and business purchases.

BUSINESS EMAIL COMPROMISE (BEC) SCAMS

BBB SCAM TRACKER BUSINESS EMAIL COMPROMISE REPORTS

SCAM TYPE	REPORTS	MEDIAN LOSS
BEC	210	$550

Source: BBB Scam Tracker (2021-2024, Q1)

More than 200 BBB Scam Tracker reports on BEC have been filed since 2021, but the number of BEC scams is likely higher. In a recent ransomware bust, the FBI found only 20% of the cybercrime's victims had reported their issue to the authorities.

Some of the toughest scams to deal with come when a fraudster impersonates someone's superior at work. **Dawn** in North Adams, Massachusetts told BBB she received an email from her boss with an invoice attached. In the message, he asked her to pay $4,500 by wire transfer. Dawn did so and emailed him to say the task was complete. Her boss immediately called her, saying he never asked her to pay for anything.

"I was confused because we had talked about paying it previously," Dawn said. "I didn't notice the email address was a junk email address and not my boss."

Mandiant Intelligence, a part of Google's cloud security team, recently released its annual report on cybersecurity called M-Trends. In that report, which primarily focused on organizational breaches, the most targeted businesses were in the financial, professional, high tech and hospitality industries. Almost one-fifth of the cases involved phishing, and over half were financially motivated, while the remaining cases centered out of China involved espionage.

Luke McNamara, Deputy Chief Analyst at Mandiant, says evolving scam tactics mean businesses need to change their defense. He said prior advice to be wary of the sender is still important, but it is now incomplete because so many scams come from the actual, compromised email addresses of CEOs, finance departments and vendors. Even instant messaging services used within organizations have been hacked, he said.

The overall numbers related to phishing do show some promise, McNamara said, as the average time to detection in Mandiant's report suggests better security practices, also known as "organizational maturity." No matter the changes organizations make, he said scammers will continue to evolve as well.

SMISHING & VISHING

While traditional phishing may have originated over email, similar scams done over text (also known as SMS messaging) are referred to as smishing. Common types of texts involve account notices, prize notifications and impersonation of delivery services.

Jim in Wenatchee, Washington told BBB he received a text message claiming to be the United States Postal Service, reaching out about a package he sent.

The text read, ***"2 delivery attempts were made, but delivery failed due to insufficient address. Please confirm your details, otherwise package will be returned to you"***. A link was attached at the end of the message.

BBB Tip: If a business or government agency you interact with texts you, confirm the alert elsewhere before responding.

Other impersonation phishing scams reported to BBB Scam Tracker included dozens of companies. An analysis of BBB data showed some businesses which had their brands stolen repeatedly included Chase Bank, Walmart and State Farm. "Wrong number" scam variations appear immensely popular as well. Smishing is one of the fastest growing types of phishing, analysis also shows. It has increased every year since 2021, according to BBB Scam Tracker, and outside research agrees, with one report showing that 39% of all mobile phishing attempts were smishing related.

While many phishing scams hope for a momentary lapse in judgment when clicking on a link, vishing scams (or voice phishing) involve the fraudster impersonating someone on the phone.

In these cases, the scammer might call someone and ask them to verify their account information. Or they may pretend to be a government official trying to gain sensitive information. At times, vishing is combined with traditional phishing or smishing to initiate contact.

In any case, the fraudster uses the leverage of already having someone on the phone to convince them, often in more persuasive ways.

Kathryn in Hemet, California told BBB in April she received a call from a man claiming to be from the Social Security Administration. He said her Social Security number had been compromised and used in various crimes involved in drug trafficking. The man used an urgent tone, telling Kathryn time was limited.

"In order that all my savings not be seized during the investigation and trial, I needed to safeguard my money in a government vault," she said.

She completed a series of Bitcoin deposits, bought gift cards and made nine wire transfers before she realized she was being defrauded. In the end, she lost $400,000.

BBB Tip: Government agencies will never ask you to move funds as part of an investigation**.**

PHARMING, MALWARE & ASSOCIATED OFFSHOOTS

In recent years, phishing has evolved to include many added complications such as pharming, which almost always pairs a traditional phishing scam with either a ransomware or tech support scam.

In these scams, a target unknowingly downloads malicious software after being secretly redirected to a scammer's website.

Timothy from Columbus, Ohio told BBB in March 2024 that he thought he was visiting Microsoft's website. After doing so, his computer locked up and was unusable. A phone number, supposedly for Microsoft, was provided on the screen, so he called it for help. The person on the other line called himself "Jerry" and told Timothy he was hacked. To help, the man said he needed remote access on Timothy's computer.

Once it was given, the computer showed Timothy's bank account number, and the man claimed a transfer for $40,000 had been initiated to a Russian bank. Timothy needed to act quickly. The only way to stop it, the man said, was to complete a series of transfers out of his account into Bitcoin. Over the next few days, Timothy followed "Jerry's" instructions and switched the full amount to Bitcoin, sending it to a provided address.

Once Timothy's wife realized what had happened, she set up an appointment with their bank, who told them it was fraud. The $40,000, however, was already lost. In these types of cases, scammers make scary sounding threats.

Donna in Caldwell, Idaho told BBB her computer froze one day. A scammer reached out and said: "I have already been watching you for some time now and have been able to contaminate your system with malware."

They claimed to have complete control of her computer and access to personal files and information. The fraudster also claimed to have used her own webcam to record Donna secretly. They threatened to spread her personal information if she didn't pay $1,300.

BBB Tip: Security experts will never ask you to transfer money to Bitcoin to safeguard it. Malvertising (malicious software embedded within advertisements online) and QR code phishing are two more common wrinkles similar to pharming.

In Springtown, Texas, **Hilda** told BBB she saw a video on YouTube supposedly posted by Elon Musk. The Musk imposter claimed he wanted to share some of his fortune and would double any funds sent to him through a QR code. Hilda scanned the code and sent $36,000.

"I sent my Bitcoin and never got anything back," she said.

Cryptocurrency was used in more than 200 reports to BBB Scam Tracker. BBB previously wrote about the digital currency's role in scams, which has increasingly played a part in international fraud.

BBB Tip: Celebrities rarely endorse or participate in direct money giveaway.

Patty in Gaithersburg, Maryland told BBB she clicked on an advertisement online, and a huge message popped up on her screen. It said she needed to call Microsoft, because her computer had been flagged for illegal searches. A number was provided.

The person on the phone said the issue was due to her accounts being compromised, including her bank at Capital One. To protect her assets, they connected her with someone who claimed to be with her bank. That supposed employee instructed her to wire $50,000 in Bitcoin through an ATM.

"They also installed a remote viewing application on my computer," Patty said to BBB. Eventually she grew suspicious and cut off contact. She couldn't recover her funds, however.

"They continue to call me to try to initiate additional transactions."

PROSECUTIONS & ACTIONS TAKEN AGAINST PHISHING SCAMS

Authorities within the United States, as well as internationally, have cracked down on phishing schemes, especially BEC scams, over the last few years.

In April 2024, a Nigerian national pleaded guilty to his role in a BEC scam which stole more than $15 million from a university in North Carolina, local government entities in Texas, construction companies and a Houston-area college. A second Nigerian national was convicted in May of a similar BEC fraud where losses totaled more than $6 million.

A man formerly from Princeton, New Jersey was indicted on 29 counts in an alleged multi-million-dollar scheme, with 14 counts of wire fraud, one count of conspiracy to commit wire fraud, one count of securities fraud, three counts of aggravated identity theft, nine counts of money laundering and one count of engaging in unlawful money transactions.

And earlier in January, a Florida man was sentenced to 51 months (about four and a half years) in federal prison for his role in laundering more than $1 million in a BEC scam. A Calgary man was charged in a multi-year email fraud investigation, in which the Royal Canadian Mounted Police said he stole more than $54,000 from a business. In Europe, 30 people were arrested for their alleged involvement in various scams that included BEC.

As law enforcement agencies have increased prosecution efforts, they have also stepped up their initiatives to proactively deal with scams as well. The FBI reported its Financial Fraud Kill Chain, an effort to freeze funds wired to scammers, put nearly $540 million of funds on hold and prevented them

from being transferred to fraudsters. That effort represented a 71% success rate in more than 3,000 cases reported to the agency.

And not all sources show a marked increase in phishing scams, however. IC3 received nearly 300,000 phishing scam reports last year, which was a 7% decrease from the previous year.

RECOMMENDATIONS TO REGULATORS

- **Expand efforts like the Financial Fraud Kill Chain, which allows institutions to freeze funds previously seen as unrecoverable.**
- **Continue to search for the purveyors of BEC scams, since the large transfers of money often provide more concrete investigative trails.**
- **Encourage AI companies to strengthen safeguards on their systems to prevent clones and other malicious copies of their software for use in scams.**

RED FLAGS & TIPS

Phishing scam red flags - watch out for an email, text message or call that:

- Claims suspicious activity or fraudulent logins
- Describes unexpected problems with an account
- Tries to confirm financial information
- Requests to click a link to make a payment
- Sends coupons unsolicited
- Generic message paired with logo of a well-known company
- Uses typo-filled and urgent language
- Offers government refunds

How businesses can protect themselves:

- Avoid or double check unknown invoices sent to email
- Be wary of sudden requests to confirm financial information
- Check email addresses from trusted partners to avoid spoofs
- Implement multi-factor authentication for all payment processes to vendors
- Train employees on how to spot and avoid phishing scams
- Create policies around best practices

Tips to strengthen cybersecurity against phishing attacks:

- Allow your cell phone to update automatically
- Turn on multi-factor authentication for sensitive accounts
- Back up your data
- Download the latest security software for your devices

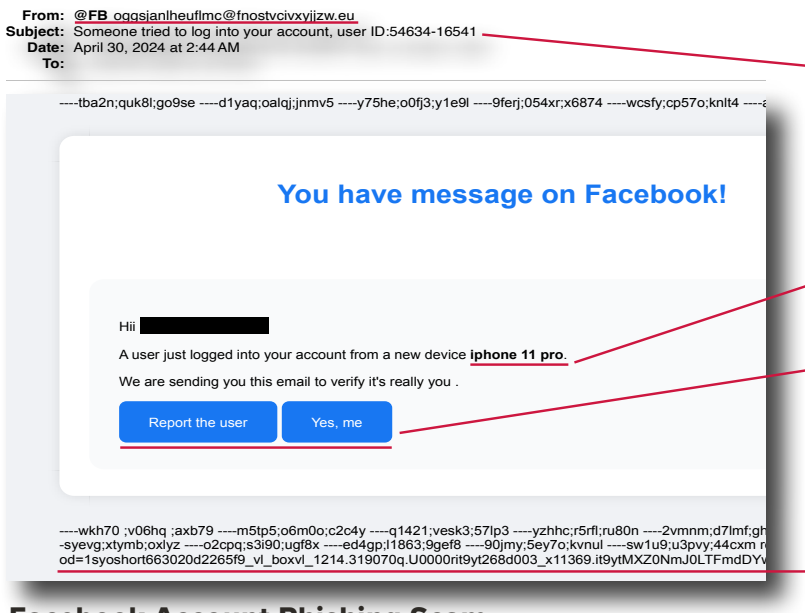
What to do if you have been subject to a phishing scam:

- If an online account is involved, immediately go to the legitimate website and change your password
- If the compromised password is used elsewhere, reset those accounts as well
- Enable multi-factor authentication
- Mark the sender as spam
- Report the fraud to various authorities

Where to report:

- Better Business Bureau or BBB Scam Tracker
- Federal Trade Commission (FTC) or call **877-FTC-Help**
- Federal Bureau of Investigation (FBI) or call **(202) 324-3000**
- Canadian Anti-Fraud Centre - or **1-888-495-8501**
- Find your state's Attorney General online

ANATOMY OF A PHISHING SCAM



Watch for non-official email domains, a hallmark of phishing scams.

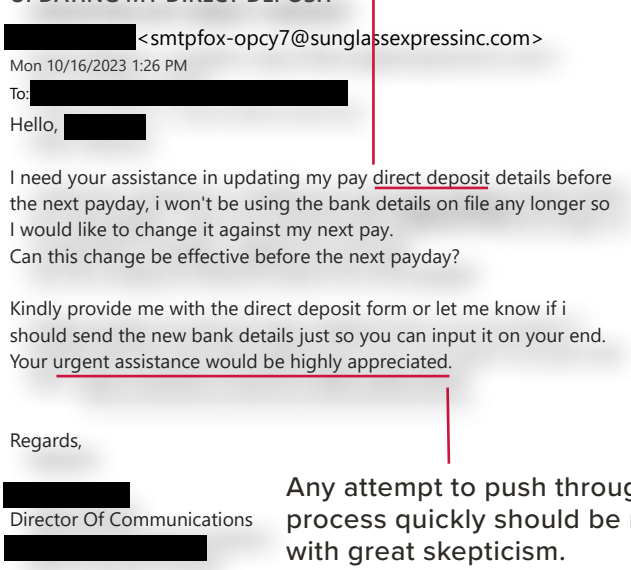
Scammers guess at personal details about you, to make the fraud more believable if they guess correctly.

Do not click! These buttons could lead to malicious software or attempts to steal personal information.

Fraudsters often have non-sensical text throughout their phishing attacks.

Facebook Account Phishing Scam

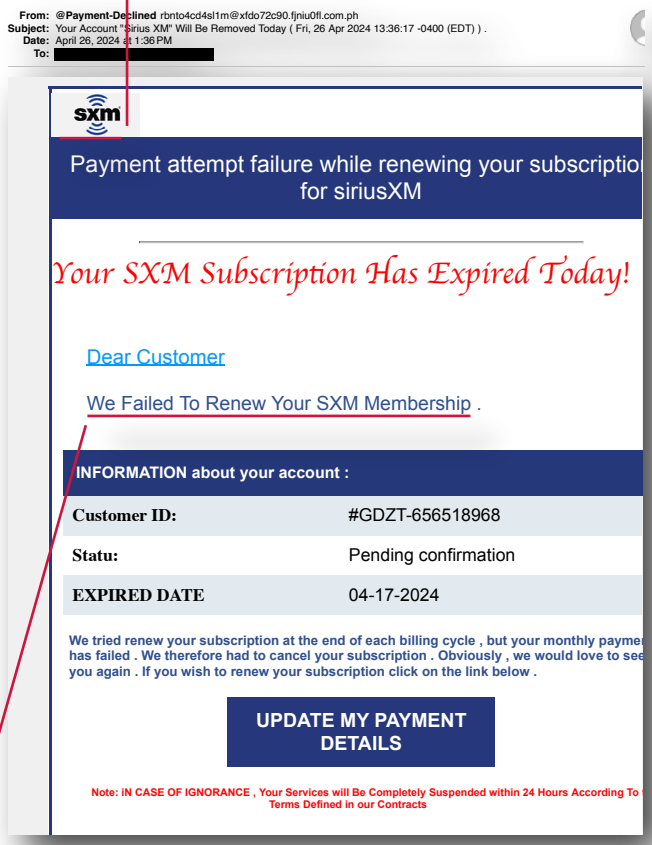
While not all in-company emails about direct deposit are scams, you should be incredibly wary. Check with the employee over another method of communication to ensure that they are the originator of an email.



Any attempt to push through a process quickly should be met with great skepticism.

HR Phishing Attack

Scammers steal official logos. Familiar letterhead doesn't mean an email is legitimate!

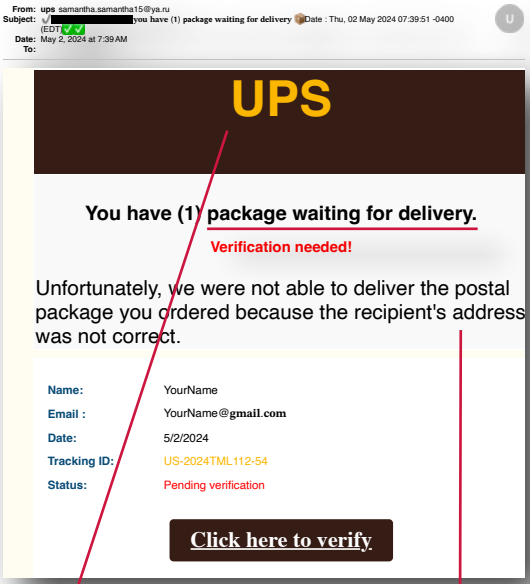


Sirius XM Phishing Scam

Urgent messages should be ignored. Fraudsters try to create a sense of urgency in their scams.

ANATOMY OF A PHISHING SCAM

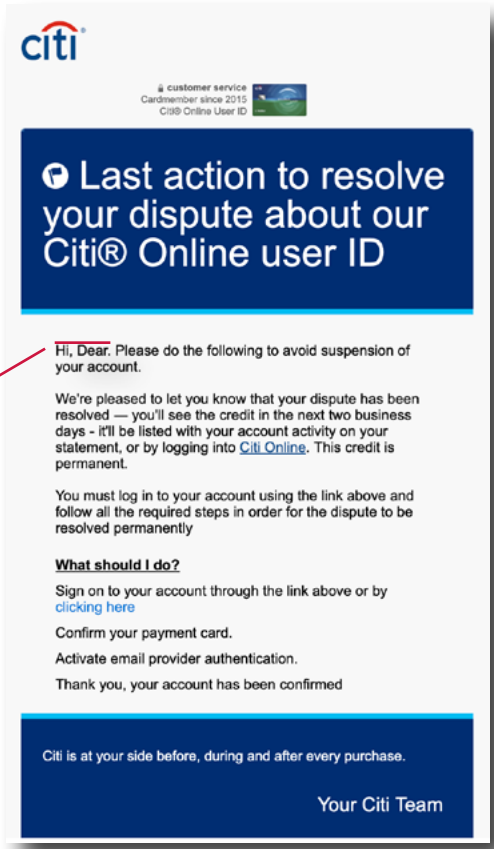
UPS Shopping Phishing Scam



Logos aren't the only things scammers steal. They imitate brands' color guides and styling as well.

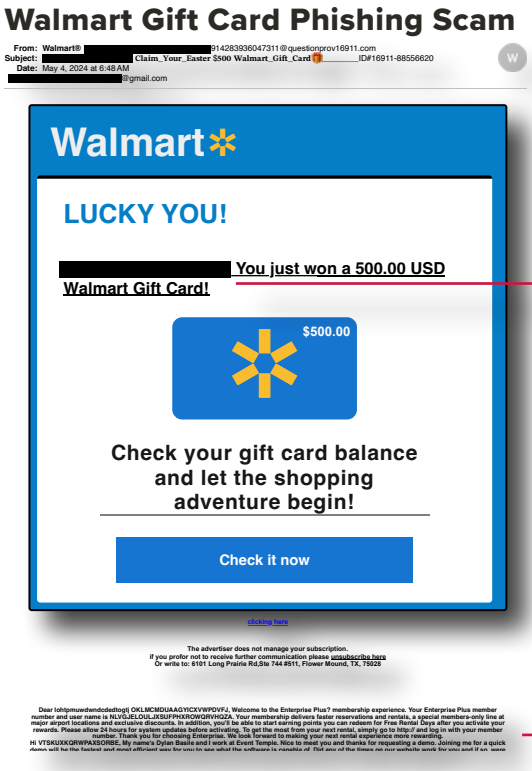
Subject lines from scammers try to grab your attention. Proceed cautiously if an unexpected email creates a sudden sense of a needing to complete a task.

Citibank Phishing Scam



Some phishing scams have evolved to mirror an official email very closely. Look for small discrepancies.

Walmart Gift Card Phishing Scam



Sometimes, an offer is too good to be true, especially when it comes to winning large sums of money unexpectedly.

If an email has a non-sensical mix of information, then scammers rushed to send out an email to a large group of people. Ignore it!

Acknowledgements

This study is a joint project of Better Business Bureaus of Chicago, Dallas, Omaha, San Francisco and St. Louis.

Contributions include data from
BBB Scam Tracker, BBB Institute for Marketplace Trust, IABBB and various regulatory agencies.

BBB International Investigations Initiative
- BBB Chicago - bbbinfo@chicago.bbb.org
- BBB Dallas - info@nctx.bbb.org
- BBB Omaha - info@bbbinc.org
- BBB San Francisco - info@bbbemail.org
- BBB St. Louis - bbb@stlouisbbb.org

By Brian Edwards, **BBB International Investigations Specialist** - bedwards@bbbinc.org

Find more information about this study and other BBB scam studies at **BBB.org/scamstudies**.

BBB's mission is to be the leader in advancing marketplace trust. We do this by:
- Setting standards for marketplace trust
- Encouraging and supporting best practices by engaging with and educating consumers and businesses
- Celebrating marketplace role models
- Calling out and addressing substandard marketplace behavior
- Creating a community of trustworthy businesses and charities

Image Credits: Getty Images

"Anatomy of a Phishing Scam" artifacts include actual screenshots of fraudulent activity.

BBB