Fraud Awareness Information

Protect Yourself Digitally

Contact Us to Learn More

Email Phishing

Bitcoin Scams

Payment App Scams

Social Media Scams

Tech Support Scams

Car Buying Scams

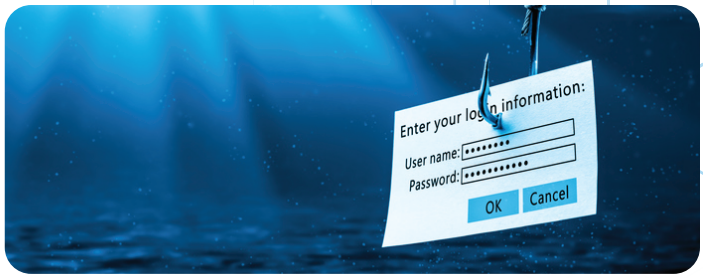
BankFinancial[SM]

1.800.894.6900 | BankFinancial.com

Member FDIC

FRAUD AWARENESS

Email Phishing Scams



It's important to stay vigilant about email scams and phishing scams to protect yourself. Here are some common scams to be aware of:

Phishing Emails: These emails attempt to trick recipients into revealing sensitive information like passwords, credit card numbers, or social security numbers. They often impersonate legitimate organizations, such as banks or popular online services, and request personal information or ask users to click on malicious links.

Nigerian Prince Scam: This is a classic scam where scammers claim to be a wealthy individual or a government official from Nigeria or another country, promising a large sum of money in exchange for a small fee or personal information.

Lottery Scams: These scams inform recipients that they have won a large sum of money in a lottery, even though they may not have participated. The scammers then ask for personal information or request payment for processing fees or taxes before releasing the winnings.

Charity Scams: Scammers exploit people's generosity by posing as representatives of charitable organizations, especially during times of natural disasters or public crises. They request donations, but the money never goes to the intended cause.

Tech Support Scams: Scammers pose as technical support representatives from well-known companies, such as Microsoft and others, to contact individuals claiming that their computer has a virus or other technical issues. They aim to gain remote access to the victim's computer or extract money for fake services.

How to protect yourself from these scams:

- Be cautious about sharing personal information or clicking on links in unsolicited emails.
- Verify the authenticity of any email requesting sensitive information by contacting the organization directly through official channels. Do not call any number listed within the email. Open a new window in your browser and Google the official company / organization's phone number and email address.
- Keep your devices and software up to date with the latest security patches.
- Use strong, unique passwords for online accounts and enable two-factor authentication whenever possible.
- Be skeptical of offers that seem too good to be true or requests for immediate action.
- Regularly monitor your financial accounts for any suspicious activity.

Remember, education and awareness are key to avoiding scams. It is best to stay informed and to report any suspicious emails or incidents to the appropriate authorities.

FRAUD AWARENESS

Bitcoin Exchange Scams

Bitcoin scams specifically targets individuals interested in investing or trading in crypto-currencies, particularly Bitcoin. Here are some common Bitcoin scams to be aware of:

Phishing Scams: Scammers send emails or direct messages pretending to be from reputable cryptocurrency exchanges or wallet providers, asking users to provide their login credentials or sensitive information. These scams aim to gain unauthorized access to users' cryptocurrency accounts.

Ponzi Schemes: Scammers promise high returns on Bitcoin investments and encourage individuals to recruit others to invest as well. However, the returns are typically unsustainable and rely on new investors' funds to pay previous investors. Eventually, the scheme collapses, and investors lose their money.

Fake Exchanges: Scammers create fraudulent cryptocurrency exchanges that appear legitimate, complete with professional-looking websites and customer support. They entice users to deposit Bitcoin or other cryptocurrencies but ultimately steal the funds or refuse to allow withdrawals.

Remember, it's important to exercise caution and conduct thorough research before engaging in any cryptocurrency-related transactions or investments.

Fake Initial Coin Offerings (ICOs): Scammers promote fraudulent ICOs, claiming to offer a new cryptocurrency or token that will yield significant profits. However, these ICOs are often scams designed to collect funds from investors without delivering any actual product or value.

Malware and Ransomware: Scammers distribute malware or ransomware that targets individuals' computers or cryptocurrency wallets. Once infected, they can steal the victims' Bitcoin or demand ransom payments in Bitcoin to restore access to their systems.

How to protect yourself from these scams:

- Be cautious about sharing personal information or clicking on links in unsolicited emails.
- Only use reputable cryptocurrency exchanges and wallet providers. Research and verify their legitimacy before providing any personal or financial information.
- Be skeptical of investment opportunities that promise unusually high returns or seem too good to be true.
- Educate yourself about cryptocurrencies and their underlying technology to better understand the risks and avoid falling victim to scams.
- Install and regularly update reliable antivirus and anti-malware software on your devices to protect against malware and ransomware attacks.
- Keep your cryptocurrency wallet software and operating systems up to date with the latest security patches.

BankFinancial℠

FRAUD AWARENESS

Payment App Scams

Payment apps such as Venmo and Zelle are digital payments services that allow users to send money to others directly from their bank accounts. Here are some general scams to be cautious of when using any digital payment service:

Phishing Scams: Scammers may send fraudulent emails, text messages, or social media messages pretending to be from Venmo, Zelle or a financial institution. These messages may ask for personal information, such as your account details or banking credentials, with the intention of stealing your identity or accessing your funds.

Overpayment Scams: In this scam, a buyer may contact you for an online sale, claiming to be interested in purchasing an item you have listed. They may send you a payment that appears to be more than the agreed-upon price and then ask you to refund the excess amount. However, the initial payment they sent may be fraudulent or reversed, leaving you out of pocket.

Purchase Scams: Scammers may pose as buyers and ask to pay for goods or services using Zelle or Venmo. They may provide fake payment confirmations or screenshots to deceive sellers into thinking they have been paid. However, no actual payment is made, and the scammer receives the goods or services without paying.

Fake Prize / Giveaways: Fraudsters send unsolicited email or text messages claiming you have won money from Venmo or Zelle. They may even ask you to take a fake survey to receive your winnings. All with the intent to lure you to a link within the message that will usually take the victim to a phishing page designed to obtain personal and Venmo or Zelle login details.

How to protect yourself from these scams:

- Be cautious of unsolicited messages or emails and avoid clicking on links or downloading attachments from unknown sources.
- Only use the official app or trusted banking apps to access the service. Avoid logging in through unfamiliar or third-party applications.
- Be skeptical of requests for personal information or banking credentials. Legitimate companies will never ask you for such details unsolicited.
- Verify the identity of the person or organization you are transacting with before sending any funds.
- Double-check payment confirmations or receipts to ensure they are legitimate before shipping goods or providing services.
- If you suspect you have encountered fraudulent activity, report it to Venmo, Zelle, your bank, and local authorities.

Remember, staying informed, using common sense, and being cautious with your personal and financial information are key to protecting yourself from scams when using digital payment services.

BankFinancial℠

1.800.894.6900 | BankFinancial.com

FRAUD AWARENESS

Social Media Scams

Over the years, Facebook has been targeted by various scams. Here are some of the top scams that have been observed on the platform:

Phishing Scams: Scammers create fake Facebook login pages or send deceptive messages, trying to trick users into revealing their login credentials. These scams may appear as notifications, emails, or direct messages, claiming that there is an issue with the user's account and requesting their personal information.

Impersonation Scams: Scammers create fake Facebook profiles that impersonate well-known individuals, celebrities, or even friends. They use these fake profiles to engage in fraudulent activities such as requesting money, soliciting personal information, or spreading malware.

Fake Giveaways: Scammers create posts or pages on Facebook offering giveaways or prizes in exchange for liking, sharing, or commenting on their content. These scams aim to collect personal information, increase engagement, or redirect users to malicious websites.

Advance Fee Fraud: Scammers contact users through Facebook, claiming to have a large sum of money or valuable items that they are willing to share but require an upfront fee or payment for processing or other reasons.

Romance Scams: Scammers create fake profiles, often pretending to be interested in romantic relationships. They build trust with their targets and eventually request money for various reasons, such as travel expenses or medical emergencies, but disappear once the funds are sent.

How to protect yourself from these scams:

- Be cautious of messages or posts from unfamiliar or suspicious sources. Avoid clicking on suspicious links or downloading files from unknown sources.
- Verify the authenticity of pages by looking for verified badges, checking the account's history and content, and comparing it to official sources if applicable.
- Be skeptical of requests for personal information or financial transactions. Avoid sharing sensitive info with unknown individuals or unverified sources.
- Enable two-factor authentication (2FA) on your Facebook account for an added layer of security.
- Regularly review and adjust your privacy and security settings on Facebook to control who can see your posts, personal information, and friend requests.
- Keep your computer and mobile devices updated with the latest security patches and antivirus software to protect against malware and other threats.

If you encounter a scam on Facebook, report it to Facebook through their reporting tools or contact their support. Additionally, be sure to educate yourself about current scams and stay informed about security best practices to protect yourself and others on the platform.

FRAUD AWARENESS

Tech Support Scams

Creating a sense of urgency, tech support scammers pose as technical support representatives from well-known companies, such as Microsoft and others, to contact individuals claiming that their computer has a virus or other technical issues. They aim to gain remote access to the victim's computer or extract money for fake services. Below is a list of common tech support scams that you should be aware of:

Phone Calls: Scammers pose as computer technicians from well-known companies, aiming to gain unauthorized, remote access to your computer. Once inside, they use fake diagnostic tests to convince you to pay for nonexistent issues.

Pop-Up Warnings: In this scam, a deceptive pop-up message claims there's a security problem on your computer. The message, which may contact an actual company's logo and appear to be legitimate, is designed to resemble an error notification from your operating system or antivirus software, prompting you to call a specified number to address the issue.

Emails: Scammers send emails that inform you of an account suspension and provide a link to resolve the issue. Clicking the link, however, results in the installation of a virus on your computer, allowing the scammer access to your system.

Online Ads and Search Results: Scammers invest in paid search advertising to promote their fake tech support services. When you call, they impersonate well-known companies, convincing you to pay for their services while potentially stealing your information, either over the phone or through malicious software.

How to protect yourself from these scams:

- Refrain from granting control of your computer to unfamiliar individuals, whether through email or phone calls. Avoid sharing your personal information or allowing access to your computer.
- Do not click on links within unsolicited pop-ups or emails. These links often contain malicious viruses designed to steal your information.
- Install and regularly update your antivirus software to enhance your computer's security.
- Recognize that legitimate tech companies do not typically reach out via email, text messages, or phone calls to notify you about computer security issues. Be cautious when such communication occurs.

Remember, it's important to safeguard your online security by not allowing strangers access, protecting your computer against viruses, and not falling prey to unfamiliar phone and email solicitations that may request computer access through suspicious links or by gathering your personal information.

To report a tech support scam, visit **ReportFraud.ftc.gov**

BankFinancial℠

1.800.894.6900 | BankFinancial.com

FRAUD AWARENESS

Car Buying Scams

Here are some of the top car buying scams to watch out for:

Title Washing: This scam involves altering a car's title to conceal its true history, such as removing information about previous accidents, flood damage, or salvage status. Sellers may present the vehicle as clean and in good condition, misleading buyers about its true value and potential problems.

Odometer Fraud: Scammers tamper with or roll back the mileage on a car's odometer to make it appear less used and more valuable. This deception can lead buyers to pay a higher price for a vehicle that has actually experienced more wear and tear.

Online Vehicle Scams: Fraudsters create fake online listings for vehicles at attractive prices to lure unsuspecting buyers. They may request upfront payment or a deposit without providing any vehicle or may claim to be located in a different country, making it difficult for buyers to inspect or receive the car.

Escrow Scams: Scammers pose as intermediaries or recommend using an escrow service to handle the transaction. They instruct buyers to wire money to the escrow account but disappear once the payment is made, leaving the buyer without the car or the funds.

VIN Cloning: In this scam, thieves use a legitimate vehicle's identification number (VIN) and transfer it to a stolen car of a similar make and model. This makes the stolen vehicle appear legitimate, and unsuspecting buyers may unknowingly purchase a stolen car.

Spot Delivery Scam: Some dealerships employ unethical tactics during the car buying process. They allow buyers to take the vehicle home before financing is approved and later inform them that the financing fell through. The buyer is then pressured into accepting unfavorable terms or paying a higher interest rate.

How to protect yourself from these scams:

- Research the vehicle's history using services like Carfax to identify any potential issues or discrepancies.
- Physically inspect the car or hire a trusted mechanic to perform a pre-purchase inspection, paying attention to the condition, mileage, and signs of damage or repairs.
- Be cautious when buying cars online and insist on seeing the vehicle in person before making any payments.
- Verify the seller's identity and contact information and be wary of dealing with sellers who refuse to meet in person or provide insufficient details.
- Never wire money or provide payment in advance without thoroughly inspecting the vehicle and ensuring all paperwork is in order.
- Check the VIN on the car's title, registration, and dashboard to ensure they match.

By staying informed, conducting due diligence, and exercising caution, you can significantly reduce the risk of falling victim to car buying scams.