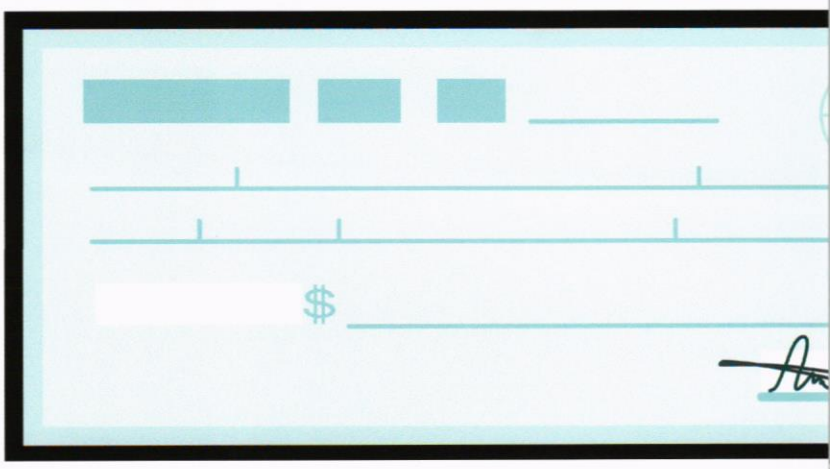
UNITED STATES POSTAL INSPECTION SERVICE

www.uspis.gov

HOW TO PREVENT
CHECK FRAUD

The United States Postal Inspection Service is the federal law enforcement branch of the United States Postal Service®. Postal inspectors are federal agents charged with enforcing over 200 federal statutes that protect the Postal Service, its employees, and the U.S. Mail™ from illegal and or dangerous use.

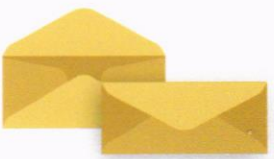


18 U.S. CODE § 1344 BANK FRAUD: Shall be fined not more than $1,000,000 or imprisoned not more than 30 years.

PROTECT YOUR MAIL
FROM MAIL THEFT AND CHECK FRAUD:

Get your mail promptly after delivery. Don't leave it in your mailbox overnight.

Contact the sender if you don't receive mail that you're expecting.



If you're heading out of town, ask the post office to hold your mail until you return.

Consider buying security envelopes to conceal the contents of your mail.

Sign up for informed delivery at USPS.com. It sends you daily email notifications of incoming mail and packages.

Use the letter slots inside your Post Office to send mail.

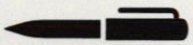
www.uspis.gov | 1-877-876-2455

ICBA

UNITED STATES POSTAL INSPECTION SERVICE

www.uspis.gov

HOW TO PROTECT YOUR CHECKS

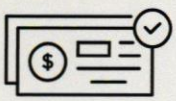


Use pens with indelible black ink so it is more difficult for a criminal to wash your checks.

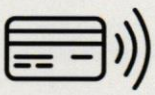
Don't leave blank spaces in the payee or amount lines.

Don't write personal details, such as your Social Security number, credit card information, driver's license number or phone number on checks.

Use mobile or online banking to access copies of your checks and ensure they are not altered. While logged in, review your bank activity and statements for errors.



If your bank provides an image of a paid check, review the back of the check to ensure the endorsement information is correct and matches the intended payee, since criminals will sometimes deposit your check unaltered.



Consider using e-check, ACH automatic payments and other electronic and/or mobile payments.

Follow up with payees to make sure that they received your check.

WHAT TO DO IF YOU'RE A VICTIM?

- Report to your local community bank and request copies of all fraudulent checks. Your community bank is your ally in helping you avoid or recover from check fraud.

- If mailed, provide details (How, When, Where). These details matter to help ***us*** determine the point of compromise in the mail stream.

- Provide law enforcement with copies of checks and details about Bank of First Deposit (BOFD) for all stolen/ altered and counterfeit checks.

www.uspis.gov | 1-877-876-2455

ICBA

Invoice Scams on the Rise

The holiday season brings excitement, along with a surge in shopping, online orders, and business transactions. Unfortunately, it's also prime time for scammers, who know that busy shoppers and companies can easily miss red flags among the flurry of invoices and delivery confirmations. As you gear up for the holiday season it's crucial to know what to watch out for to avoid becoming a victim of these costly schemes. Here's a quick guide to help you spot fake invoices and stay safe this season.

Know How Fake Invoices Work

Fake invoices have become increasingly sophisticated, with scammers crafting invoices that look legitimate. These often feature familiar company logos and realistic details to deceive people into paying for items or services they never ordered. During the holiday season, scammers know that businesses and individuals are handling a high volume of purchases and orders, making it easy to overlook small discrepancies.

Common Tactics Include:

- ***Bogus Delivery Notifications*:** "Missed delivery" emails or texts prompt you to pay a fee to reschedule or confirm delivery.
- ***Phishing Emails From "Trusted Brands":*** Scammers use fake invoices appearing to be from major brands or online retailers. These often include a fake support number the scammer hopes you'll call.
- ***Subscription Renewal Scams:*** These invoices warn you of "impending charges" for services like software or memberships unless you cancel (by giving away personal info).

Signs of a Fake Invoice

- ***Unfamiliar Vendor Names:*** If you don't recognize the vendor, do some research. If you have no record of ordering from them, it's suspicious.
- ***Suspicious Contact Information:*** Legitimate companies don't ask you to reach them at random email addresses or phone numbers.
- ***High Urgency or Threats:*** Scammers use urgent language to pressure you into acting fast, like claiming your account will be suspended or cancelled.
- ***Errors in Details or Spelling:*** Even the most professional-looking invoice can have odd language, typos, or minor formatting issues.

Steps to Take if You Suspect a Fake Invoice

- ***Don't Click Links or Download Attachments:*** These may contain malware or phishing attempts. Instead, go directly to the company's official website if you need to check an order.
- ***Report It:*** If you've received a fake invoice, report it with your email or text provider. You can also report phishing scams to the Federal Trade Commission (FTC).
- ***Stay Organized:*** Keep a record of orders and purchases, especially during the holidays. A simple list in your phone or planner can help you spot unauthorized charges.

Phishing: Don't Take the Bait

Phishing is when you get emails, texts, or calls that seem to be from companies or people you know. But they're actually from scammers. They want you to click on a link or give personal information (like a password) so that they can steal your money or identity, and maybe get access to your computer.

The Bait

Scammers use familiar company names or pretend to be someone you know.

They ask you to click on a link or give passwords or bank account numbers. If you click on the link, they can install programs that lock you out of your computer and can steal your personal information.

They pressure you to act now — or something bad will happen.

Avoid the Hook

Check it out.

- Look up the website or phone number for the company or person who's contacting you.
- Call that company or person directly. Use a number you know to be correct, not the number in the email or text.
- Tell them about the message you got.

Look for scam tip-offs.

- You don't have an account with the company.
- The message is missing your name or uses bad grammar and spelling.
- The person asks for personal information, including passwords.
- **But note: some phishing schemes are sophisticated and look very real,** so check it out and protect yourself.

Protect yourself.

- Keep your computer security up to date and back up your data often.
- Consider multi-factor authentication — a second step to verify who you are, like a text with a code — for accounts that support it.
- Change any compromised passwords right away and don't use them for any other accounts.

Report Phishing

- Forward phishing emails to **spam@uce.gov** and **reportphishing@apwg.org**.
- Report it to the FTC at **ftc.gov/complaint**.

For more information, visit **ftc.gov/phishing**
aba.com/phishing

ABA FOUNDATION.

Phishing Exposed: Safeguarding Your Clicks

In the ever-evolving landscape of cyber threats, phishing scams have become a very prominent weapon used by cybercriminals. These deceptive tactics prey on unsuspecting individuals by leveraging various techniques to compromise personal information, devices, and even financial assets. This week, we'll share details on common phishing tactics fraudsters use, red flags you can look for, and some tips on how to stay safe.

- **Phishing Emails:** Email remains the primary avenue for phishing attacks. Fraudsters often craft very convincing emails to impersonate reputable entities like banks, government agencies, popular online shopping platforms, and much more. These emails typically contain urgent messages, perhaps alerting you to a charge you will not recognize. These emails are designed to entice users to click on malicious links, download malicious attachments, or call phone numbers that will directly connect you with a criminal who's waiting to take control of your device.

- **Malware and Viruses:** Phishing scams frequently involve the distribution of malware and viruses. Malicious software can be hidden in seemingly harmless downloads or links, waiting to infiltrate an entire system. Once installed, malware can capture sensitive information, track keystrokes, or even take control of the entire device. Always be cautious when clicking on links or downloading attachments, especially ones you aren't expecting.

- **Information or Device Compromise:** Phishing extends beyond email, targeting users through various digital channels. Social media platforms, messaging apps, and fake websites are commonly used by fraudsters to trick victims into divulging sensitive information or even providing access to their device. To avoid a compromise, always verify the legitimacy of communication you receive before taking any action. When verifying, only use contact information you have verified on the organization's official website.

- **Fake Websites and Spoofed Domains:** Fraudsters often create fake websites that mimic legitimate ones to deceive you into providing login credentials or financial information. These spoofed domains can very closely resemble trusted sites, making it a challenge for users to discern the difference. Vigilance is crucial when entering personal information online. Always remember to check the website's URL for authenticity.

- **Text Message (SMS) Phishing:** As mobile devices play a huge role in our daily lives; fraudsters commonly exploit text messaging as another way to trick you. You may receive fraudulent text messages containing links or prompts to call a specific phone number. Like phishing emails, these messages often contain an urgent message. Clicking on the links can lead to malware installation whereas calling the phone number can lead to elaborate and very convincing social engineering attempts.

HOW TO SPOT A

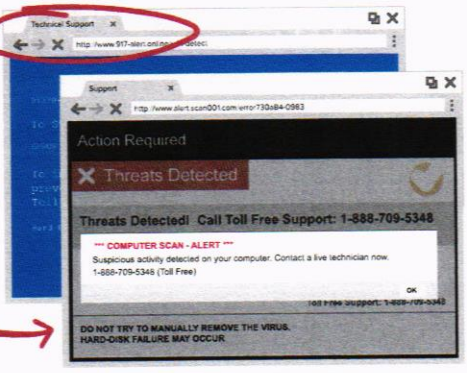
TECH SUPPORT SCAM

It often starts with a pop-up . . .

Shows up within your **internet browser**

Might **imitate** a blue error screen

or trusted antivirus software



CALL	NOW	OR ELSE...
Wants you to call a **toll-free number**	Urges you to call **immediately**	Threatens that you may **lose personal data** if you don't call

Then, you call a toll-free number. The scammer might:

- ask you to give them remote access
- pretend to run a diagnostic test
- tell you they've found a virus or other security issue
- try to sell you repair sevices or a security subscription

Then, you're asked to pay a fee.

The scammer provides "services" that range from:

WORTHLESS

- things you can get elsewhere for free
- things you already have
- "fixing" a problem that doesn't exist
- subscriptions that don't do anything
- installing malware

MALICIOUS

WHAT YOU CAN DO:

- If you get a pop-up, call, spam email or any other urgent message about a virus on your computer, **stop**.
  - Don't click on any links or call a phone number.
  - Don't send any money.
  - Don't give anyone control of your computer.
  - *Microsoft does not display pop-up warnings and ask you to call a toll-free number about viruses or security problems.*
- **Report it** at ftc.gov/complaint. Include the phone number that you were told to call.
- Keep **your security software** up to date. Know what it looks like so you can spot a fake.
- **Tell someone** about this scam. You might help them spot it and avoid a costly call.

LEARN MORE: ftc.gov/TechSupportScams

Tech Support Scams

In today's digital age, tech support scams have become a growing concern. Scammers pose as technical support representatives, targeting unsuspecting individuals to gain access to their personal or financial information and computer systems. It's very important to protect yourself from these scams, as they often lead to device compromise, identity theft, and monetary loss. Tech support scams are a real threat, but by remaining vigilant and staying educated, you can protect yourself from falling victim to these deceptive tactics. Here are some key points and best practices that will help you stay safe:

1. **Recognize the signs:**
    - Unsolicited calls: Be cautious of unexpected phone calls claiming to be from reputable tech companies, like Microsoft. Legitimate companies rarely contact customers directly.
    - Pop-up messages: Beware of alarming pop-up messages on your computer or web browser claiming that your system is compromised. These often include bogus contact details to trick you into calling the scammers.
    - Urgency and fear tactics: Scammers may create a sense of urgency, emphasizing the severity of the issue and pressuring you to act immediately. They intend to catch you off guard and to prevent you from verifying their claims.
2. **Avoid providing remote access:**
    - Do not grant remote access to your computer or device unless you initiated the request and are dealing with a trusted professional that you know. Scammers will use this access to install malware, steal your personal or financial information, or even to hold your system hostage for a ransom.
3. **Verify the representative's authenticity:**
    - Ask for identification: Legitimate tech support representatives will gladly provide their full name, employee ID, and contact details. Take note of this information for future reference.
    - Call back using only official contact information: If you're unsure about a caller, independently look up the company's' official contact information and use it to call them back. Do not rely on contact details provided by a caller, in correspondence, or phone numbers found with a simple search. Always visit the company's official website to find this information.
4. **Safeguard your personal and financial information:**
    - Never share sensitive information: Legitimate tech support representatives will **NEVER** ask you for credentials or to provide (or access) your financial information, nor will they ask for your social security number over the phone or by email.

Did someone tell you to buy a gift card and give them the PIN numbers?

STOP. It's a scam!

Gift cards are only for gifts.
Not for payments.

HANG UP ON Gift Card Scams

- Report gift card scams to the gift card company.
- Ask for your money back.
- Then tell the FTC at

ReportFraud.ftc.gov

Did someone tell you to buy a gift card and give them the PIN numbers to:

- pay the FTC, FBI, or IRS
- keep your Social Security benefits
- keep your utilities on (electricity, water, or heat)
- pay for tech support
- help a family member in trouble
- help a servicemember needing money
- pay bail or ransom
- avoid arrest or deportation
- fix **any** problem, for any reason?

If you answered yes, HANG UP. It's a scam.

- Report gift card scams to the gift card company.
- Ask for your money back.
- Then tell the FTC at **ReportFraud.ftc.gov**

Contact the gift card company:

Amazon
(888) 280-4331

Apple iTunes
(800) 275-2273

Ebay
ebay.com/giftcardscams

Steam
help.steampowered.com

Target
(800) 544-2943

Walmart
(888) 537-5503

Learn more about gift card scams: **ftc.gov/giftcards**

Did you recently get a notice that says your personal information was exposed in a data breach? Did you lose your wallet? Or learn that an online account was hacked? Depending on what information was lost, there are steps you can take to help protect yourself from identity theft.

If your information has been exposed, visit IdentityTheft.gov/databreach for detailed advice about your particular situation.

Depending on the type of information exposed, the next page tells you what to do right away. You'll find these steps – and more – at **IdentityTheft.gov/databreach**.

What information was lost or exposed?

Social Security number

- ☐ If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- ☐ Get your free credit reports from **annualcreditreport.com**. Check for any accounts or charges you don't recognize.
- ☐ Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name.

  If you decide not to place a credit freeze, at least consider placing a fraud alert
- ☐ Try to file your taxes early – before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job.

Online login or password

- ☐ Log in to that account and change your password. If possible, also change your username

  If you can't log in, contact the company. Ask them how you can recover or shut down the account.
- ☐ If you use the same password anywhere else, change that, too.
- ☐ Is it a financial site, or is your credit card number stored? Check your account for any charges that you don't recognize.

Bank account, credit, or debit card information

- ☐ If your bank information was exposed, contact your bank to close the account and open a new one.
- ☐ If credit or debit card information was exposed, contact your bank or credit card company to cancel your card and request a new one.

Other information

For guidance about other types of exposed information, visit **IdentityTheft.gov/databreach**.

If your child's information was exposed in a data breach, check out ***Child Identity Theft – What to know, What to do***.

FEDERAL TRADE COMMISSION
IdentityTheft.gov
September 2016

Data Breaches

What to know, What to do

FEDERAL TRADE COMMISSION
IdentityTheft.gov

Data Breach Alert: What It Means and What You Should Do

In today's digital world, data breaches seem to happen constantly. Whether it's a major retailer, a financial institution, government agency, or even a healthcare provider, companies are frequently targeted by cybercriminals looking to steal sensitive information. But what does a data breach actually mean for you as a consumer? And more importantly, how can you protect yourself?

What is a Data Breach?

A data breach occurs when hackers gain unauthorized access to sensitive information, such as:

- **Names, addresses, and phone numbers**
- **Social Security numbers**
- **Credit card or banking details**
- **Login credentials (usernames and passwords)**
- **Medical records**

Once this data is stolen, it can be sold on the dark web, used for identity theft, or leveraged in scams.

How Data Breaches Affect You

If your information is exposed in a breach, you may face:

- **Identity Theft:** Fraudsters can open credit accounts, take out loans, or file tax returns in your name.
- **Financial Fraud:** Stolen credit card numbers may be used for unauthorized purchases.
- **Account Takeovers:** Hackers may try to access your online accounts, especially if you reuse passwords.
- **Phishing and Scams:** Criminals use leaked information to craft convincing scam emails, texts, or phone calls.

How to Protect Yourself

- **Check if You've Been Affected:** Use free tools like https://haveibeenpwned.com/ to check if your email or passwords have been exposed in a breach. Many companies also notify customers when their data is compromised – always take those alerts seriously.
- **Change Your Passwords and Enable Multi-Factor Authentication:** Update passwords for any affected accounts immediately. Use strong, unique passwords for each website. Consider using a password manager to generate and store secure passwords. Adding an extra layer of security (like biometrics) makes it harder for hackers to access your accounts.
- **Monitor Your Financial Accounts and Freeze Your Credit:** Regularly review your bank and credit card statements for suspicious transactions and set up alerts for any unusual activity. If your Social Security number was compromised, consider freezing your credit can prevent criminals from opening new accounts in your name. You can do this for free with the three major credit bureaus: *Equifax, Experian, and TransUnion*.
- **Watch Out for Scams:** Be cautious of emails or calls claiming to be from companies involved in a breach. Scammers often use breached data to make phishing attempts more convincing. Never click on suspicious links or provide personal information unless you verify the source.

Protecting Your Digital Life: Safeguarding Device Management Accounts

In today's connected world, our lives revolve around smart devices, and we rely on accounts tied to companies like Google and Apple to manage them. These accounts are the gateways to our digital existence, holding sensitive information and serving as keys to unlock our devices. It's crucial to understand the risks associated with these accounts and the steps you can take to keep them safe from scammers and malicious actors.

The Risks of Compromised Device Management Accounts

- **Identity Theft:** When a scammer gains access to your device management account, they can steal personal information including your name, address, and contact details. If you've stored a photo of your ID or other documents and images containing sensitive information, they're also at risk.
- **Financial loss:** Scammers can use saved credentials to exploit your accounts and make unauthorized purchases, putting your hard-earned money at risk. Remember, any information you have stored on your device is at risk if your device management account is compromised.
- **Unauthorized Access:** Once a scammer takes control of your device management account, they can access and control your devices remotely. This can include locking you out of your own devices or even erasing your data. This also means that any calls or messages you receive could be intercepted by the scammer, including any additional security codes necessary to gain access to your most sensitive accounts.

How to Stay Safe

- **Enable Multi-Factor Authentication (MFA):** MFA adds an extra layer of security to your accounts. It typically involves receiving a one-time code on your mobile device or email that you need to enter during the login process. By enabling MFA, it will be much more difficult for scammers to gain access to your accounts, even if they have your credentials.
- **Use Strong, Unique Passwords:** Always create strong and unique passwords. Consider using a password manager to help generate and store complex passwords for each of your accounts.
- **Beware of Phishing Attempts:** Scammers often use phishing emails or fake websites to trick you into providing sensitive information. Be cautious of unsolicited emails or messages, especially if they ask for your login details or direct you to unfamiliar websites. ALWAYS verify the authenticity of the source before taking any action.
- **Regularly Review Account Activity:** Frequently check your account activity for any suspicious logins or unfamiliar devices. Most device management accounts provide activity logs that show recent login attempts and devices that have accessed your account.
- **Keep Software and Firmware Updated:** Regularly update the operating systems and firmware on your devices. These updates often contain security patches that protect against known vulnerabilities.
- **Educate Yourself and Your Family:** Ensure that everyone in your household understands the importance of account security. Educate family members and friends about the risks and precautions to take.

Stay in Control: How Debit Card Alerts & Controls Protect You from Fraud

Keeping your money safe is easier than ever with *debit card alerts and controls*. Scammers are always looking for ways to access your funds, but with the right tools, you can stay one step ahead. Many financial institutions offer features that notify you of card activity and allow you to control when and how your card is used. Here's some information on how these tools can help protect you from fraud.

- **Transaction Alerts – Know When Your Card Is Used**

  Transaction alerts notify you every time your debit card is used. Whether it's an online purchase, an in-store swipe, or even an ATM withdrawal, you'll receive notification right away. This helps you:

  - ✓ Spot unauthorized charges right away
  - ✓ Monitor your spending habits
  - ✓ Stay aware of automatic subscriptions or recurring payments

- **Card On/Off Controls – Instant Security at Your Fingertips**

  If your card is lost, stolen, or simply not in use, on/off controls let you disable it instantly. When you're ready to use it again, just switch it back on. This feature helps:

  - ✓ Prevent unauthorized transactions
  - ✓ Reduce the risk of fraud when your card isn't in use

- **Scheduled Card On/Off – Set It and Forget It**

  For even more control, several financial institutions allow you to *schedule when your debit card is active*. This means you can:

  - ✓ Disable your card at night or during hours you don't usually spend
  - ✓ Set usage limits based on your unique routine
  - ✓ Reduce the risk of unauthorized transactions while you sleep

Scammed? Don't Wait – Every Second Counts

When you realize you've been scammed, time is your best defense. Hesitating – even for a few minutes – can give criminals the head start they need to steal your money, access your accounts, or lock you out entirely. Whether you've accidentally shared your passwords, clicked a bad link, or made a payment to a scammer, acting fast can limit the damage. Here's what to do right away:

- **Secure the Affected Account Immediately** - If you entered your password on a fake website or shared login details, act fast:
  - *Change your password immediately.* Don't wait to contact support – secure the account first
  - *Use a strong, unique password.* Avoid reusing old passwords or simple combinations.
  - *Enable multi-factor authentication (MFA)* if it's available – this adds an extra layer of protection.

- **Disconnect from the Internet (If Malware Is a Concern)** – If you clicked a suspicious link or downloaded an attachment, disconnect your device from Wi-Fi or data to limit further exposure. Then:
  - *Run a trusted antivirus scan to check for malicious software.*
  - *Avoid logging back in to sensitive accounts until you're certain the device is secure.*

- **Contact the Company or Service Involved** – Whether it's your bank, email provider, or social media platform, reach out to their support team right away as many companies have 24/7 fraud hotlines. Don't delay.
  - For financial issues: *Contact your financial institution right away* to review activity and ask about placing a freeze on your account.
  - For other compromised accounts: *Notify the platform using official contact information and follow their recovery steps.*

- **Report the Scam** – Reporting the incident helps protect others and may improve your chances of recovery:
  - For financial fraud: *Contact your financial institution and the Federal Trade Commission (FTC).*
  - For hacked accounts: *Report the breach to the affected platform using official contact information.*

- **Stay Alert for Follow-Up Attacks** – Scammers may try to exploit the situation further:
  - *Watch for fake "help desk" calls claiming to fix the problem.*
  - *Be wary of follow-up emails pretending to offer refunds or solutions.*
  - *Monitor your accounts for unusual activity in the coming weeks.*