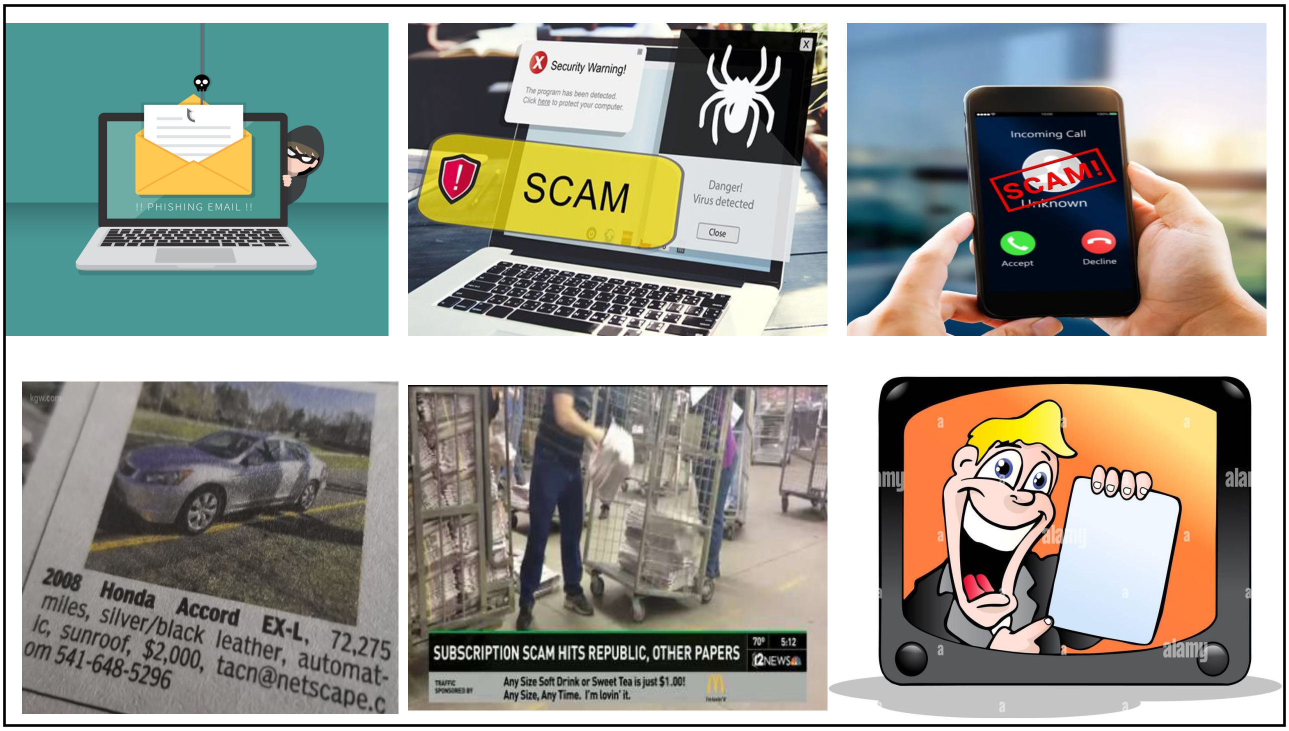

!! PHISHING EMAIL !!
Security Warning!
The program has been detected.
Click here to protect your computer.
SCAM
Danger!
Virus detected
Close
Incoming Call
SCAM!
Unknown
Accept
Decline
2008 Honda Accord EX-L, 72,275 miles, silver/black leather, automatic, sunroof, $2,000, tacn@netscape.com 541-648-5296
SUBSCRIPTION SCAM HITS REPUBLIC, OTHER PAPERS
70° 5:12
12NEWS
TRAFFIC SPONSORED BY
Any Size Soft Drink or Sweet Tea is just $1.00!
Any Size, Any Time. I'm lovin' it.

# Unleashing Scammers!

# States Should Take Them On?

by seeking to fire 90 percent of the **Consumer Financial Protection Bureau** (CFPB)'s staff, dismantling the Justice Department's National Cryptocurrency Enforcement Team and Consumer Protection Branch, and dropping or settling cases with more than 100 corporations that scammed or abused consumers, the Trump administration is instead inviting a golden age for scammers and corporate abuse.

As the federal government retreats from protecting consumers, it is up to states to step up, including through the creation of state-level CFPBs.

## What do scammers want?

**Scammers are dishonest people.**

- Liars who convince you to send them money.
- Other scammers want your information.
They try to get information like the username and password for your bank account, credit card number, and Social Security.
- They want your information so they can pretend to be you and use your accounts without permission.

**Scammers contact YOU and say there's a problem.**

They will lie and say you owe the money. They might pretend someone in your family had an emergency. They could say there's a virus on your computer. Or they might tell a different lie.

But there's no real problem or emergency — they just made it up to get your money or information.

**Scammers tell you to hurry.**

They don't want you to have time to think or to check out their story. Scammers might even lie and say you'll be arrested if you don't act quickly.

Scammers tell you to pay, and they tell you **HOW** to pay.
Scammers often say you can only pay by:

- Buying gift card and giving them the numbers on the back
- Wiring money through a company like MoneyGram or Western Union
- Sending them cryptocurrency
- Using a payment app

They tell you to pay these ways because it's like using cash. Once you pay, it's hard to get your money back.

# Warnings Signs of a Scam

**Did someone promise you a job – if you pay them?**

Never pay anyone who promises you a job, a certificate that will get you a job, or secret access to a job. Those are scams.

**Did someone say they're from a government agency, threaten you or demand money?**

The government doesn't call to threaten you or demand money.

**Did someone say they could help you win the Diversity Visa Lottery to get a Green Card?**

It's free to apply and the winners are picked at random. No one can increase your chance of winning.

Did you get a call, email, text, or social media message saying you won something? Except there's a fee?
Don't pay for a prize. That's a scam. You'll lose your money.

# Warnings Signs of a Scam

**Did someone ask you to pay by gift card, money transfer through a company like Western Union or MoneyGram, or cryptocurrency?**

Only scammers say you have to pay that way. Don’t do it.

**Did you get a check from someone who asked you to give them part of the money back?**

Don’t give someone money in return for a check. Fake checks can look real and fool the bank. You’ll have to pay back the money.

**Did you get a call, email, text, or social media message asking for your credit card, bank account, or Social Security number?**

Never give that information to anyone who asks over phone, email, text, or social media.

## Online & Smart Phone

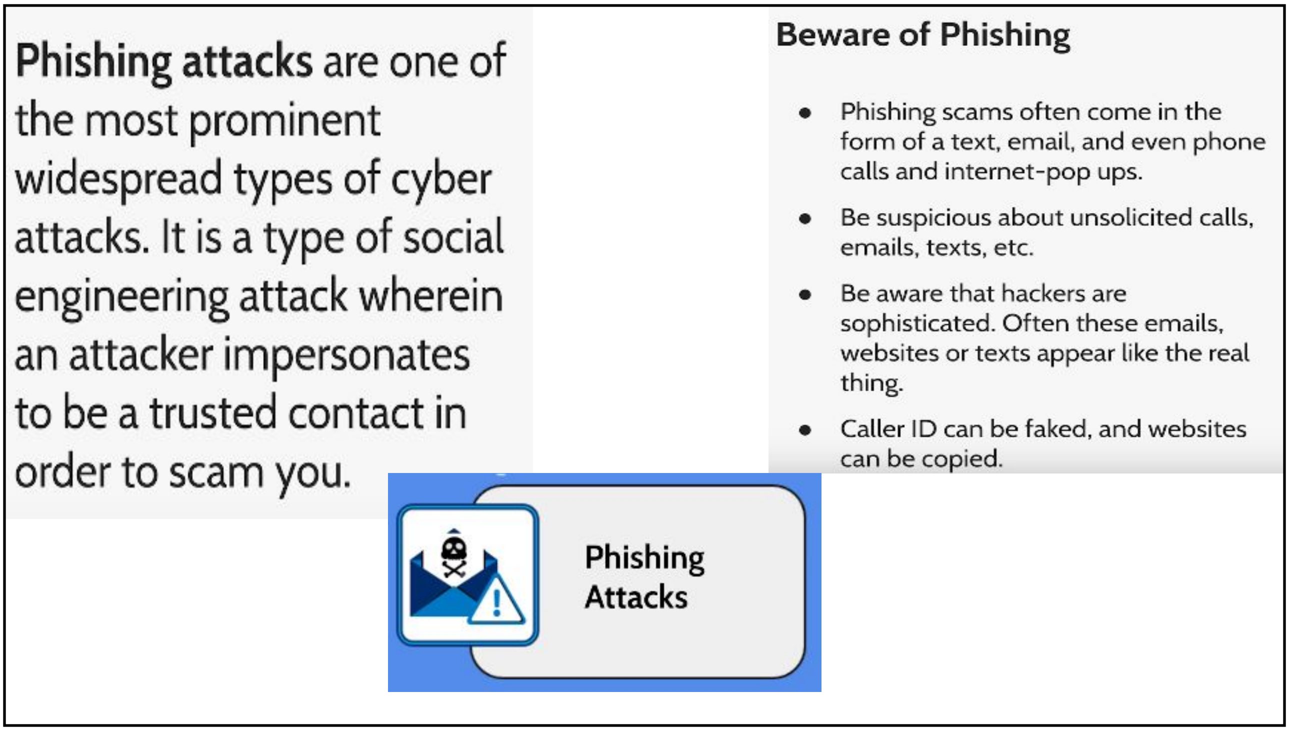
Phishing

Smishing

Man-in-the-Middle

Malware

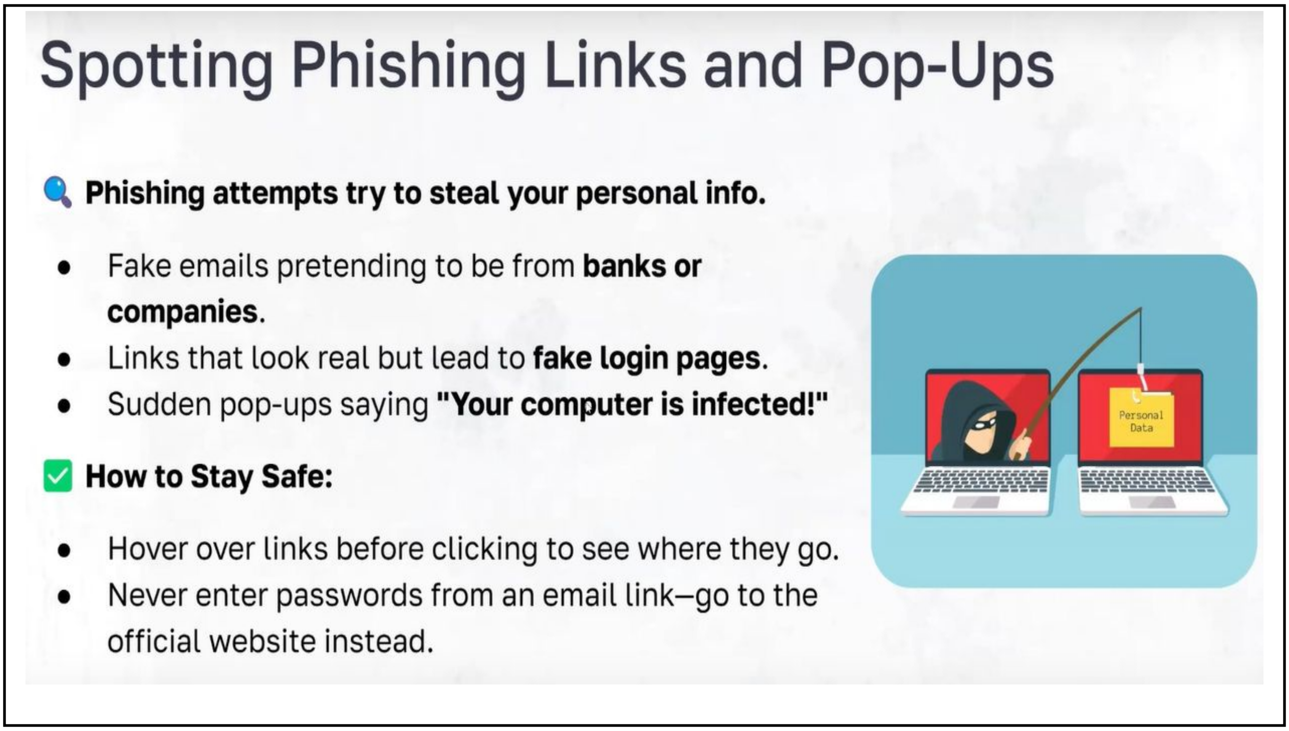
Fake Websites



**Phishing attacks** are one of the most prominent widespread types of cyber attacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact in order to scam you.

## Beware of Phishing

- Phishing scams often come in the form of a text, email, and even phone calls and internet-pop ups.
- Be suspicious about unsolicited calls, emails, texts, etc.
- Be aware that hackers are sophisticated. Often these emails, websites or texts appear like the real thing.
- Caller ID can be faked, and websites can be copied.



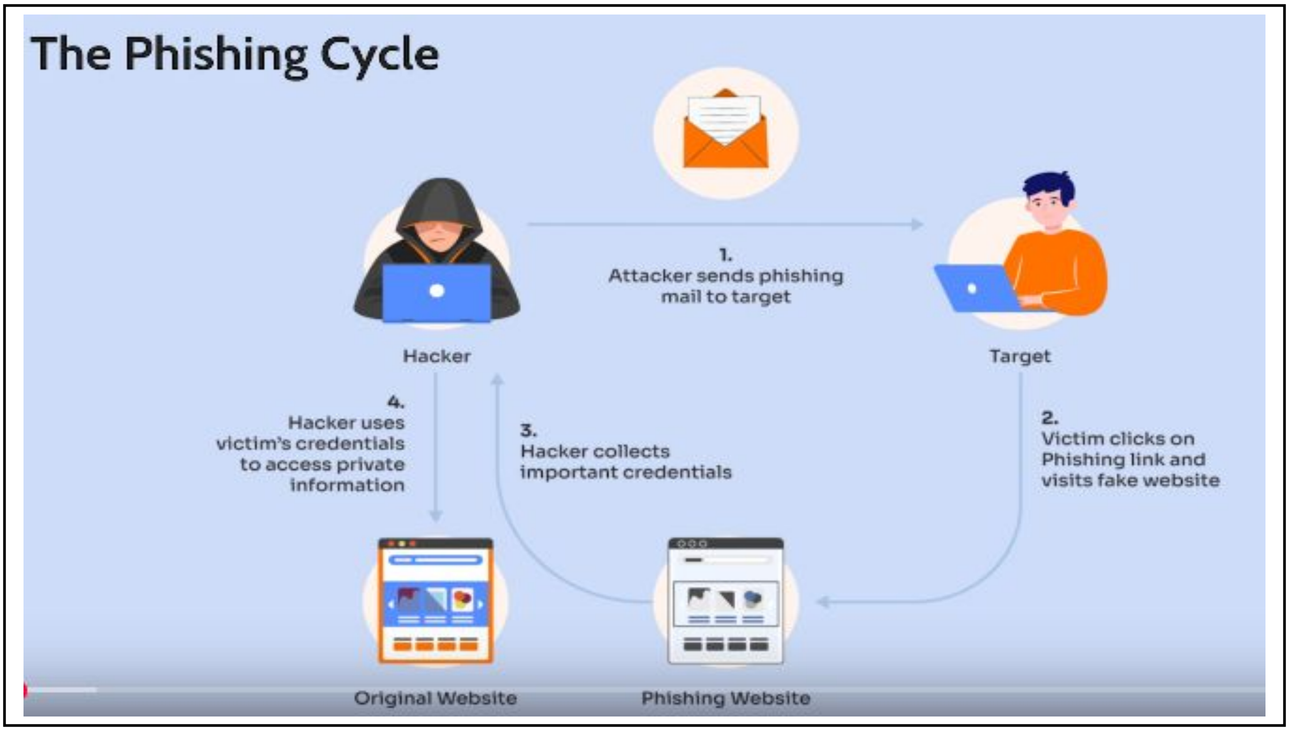
# Spotting Phishing Links and Pop-Ups

🔍 **Phishing attempts try to steal your personal info.**

- Fake emails pretending to be from **banks or companies**.
- Links that look real but lead to **fake login pages**.
- Sudden pop-ups saying **"Your computer is infected!"**

✅ **How to Stay Safe:**

- Hover over links before clicking to see where they go.
- Never enter passwords from an email link—go to the official website instead.



## The Phishing Cycle

Hacker

1. Attacker sends phishing mail to target

Target

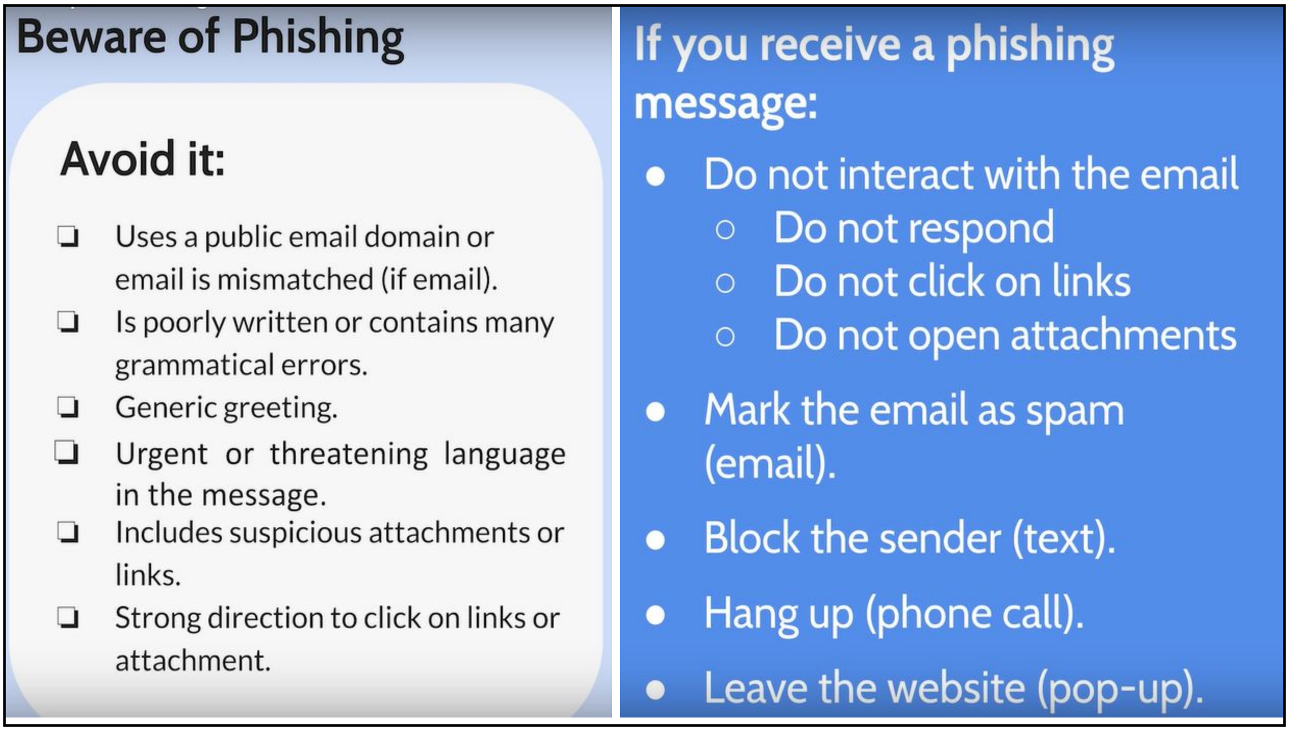
2. Victim clicks on Phishing link and visits fake website

3. Hacker collects important credentials

4. Hacker uses victim's credentials to access private information

Original Website

Phishing Website



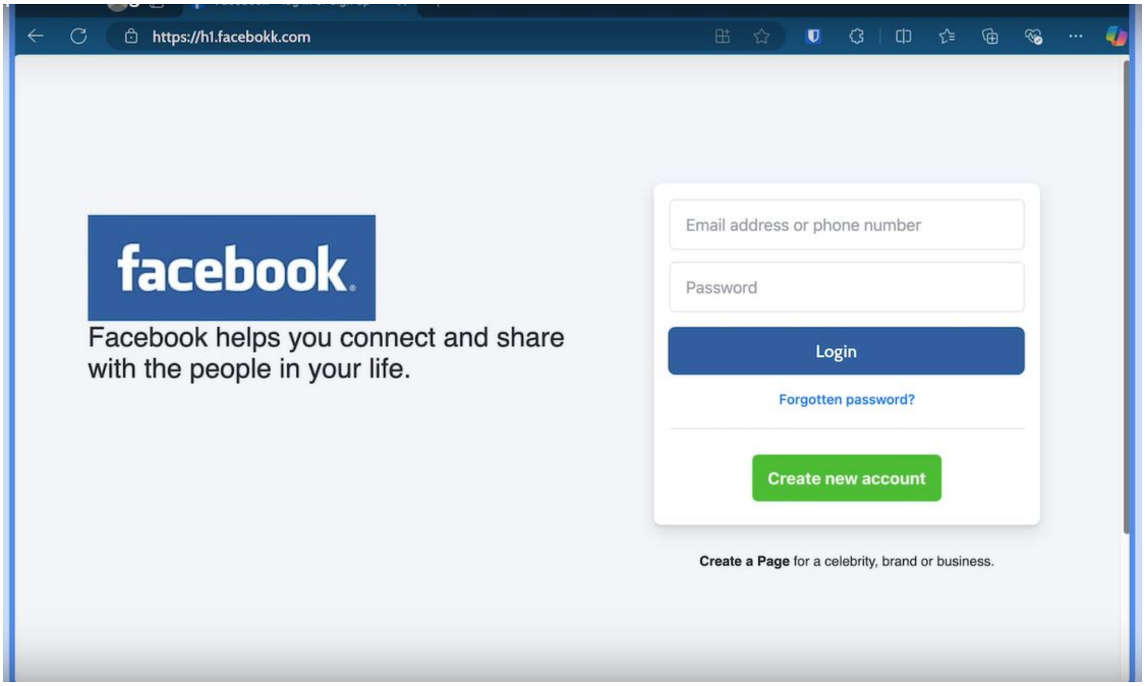
## Beware of Phishing

### Avoid it:

- ❏ Uses a public email domain or email is mismatched (if email).
- ❏ Is poorly written or contains many grammatical errors.
- ❏ Generic greeting.
- ❏ Urgent or threatening language in the message.
- ❏ Includes suspicious attachments or links.
- ❏ Strong direction to click on links or attachment.

## If you receive a phishing message:

- Do not interact with the email
  - Do not respond
  - Do not click on links
  - Do not open attachments
- Mark the email as spam (email).
- Block the sender (text).
- Hang up (phone call).
- Leave the website (pop-up).



https://h1.facebokk.com

facebook

Facebook helps you connect and share with the people in your life.

Email address or phone number

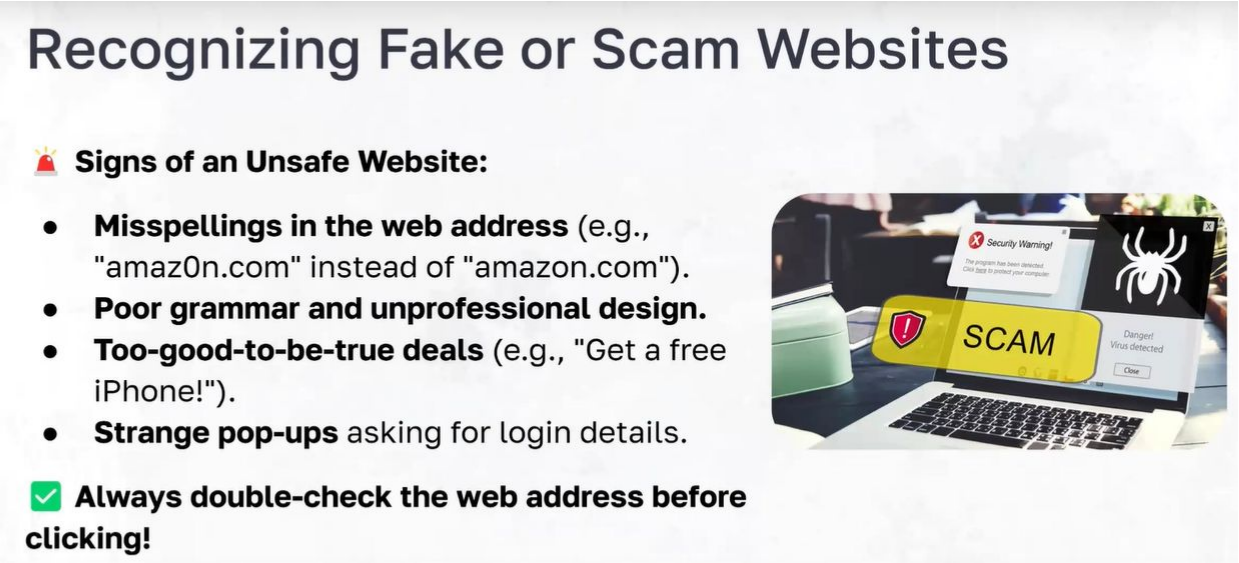
Password

Login

Forgotten password?

Create new account

**Create a Page** for a celebrity, brand or business.



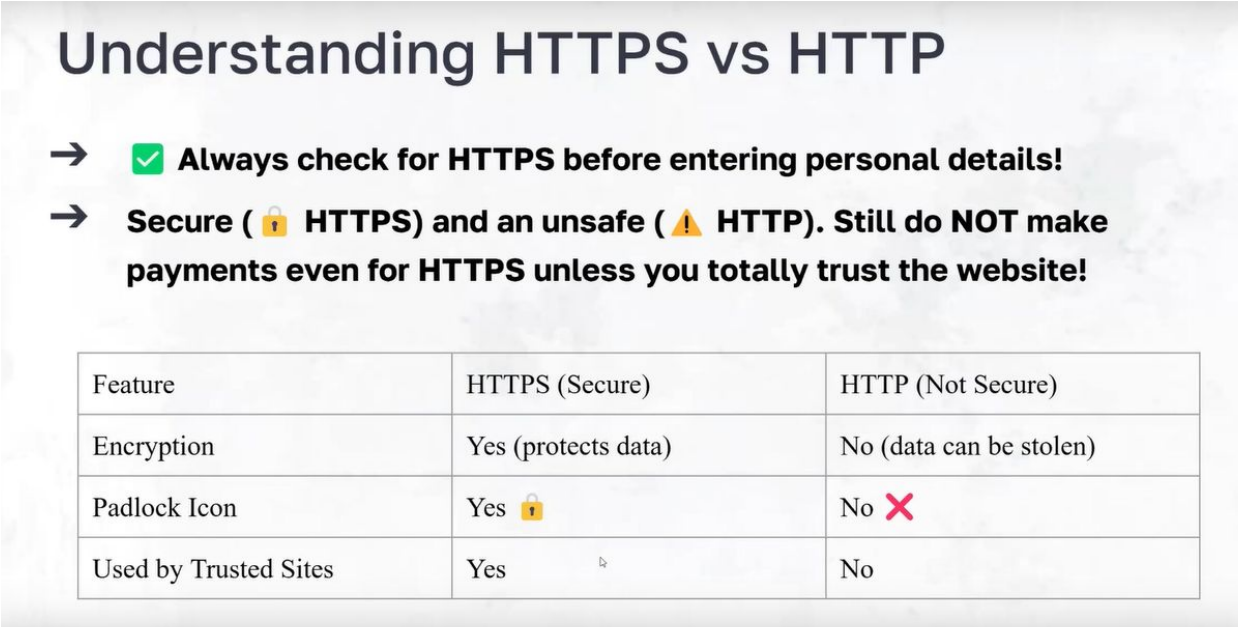
# Recognizing Fake or Scam Websites

🚨 **Signs of an Unsafe Website:**

- **Misspellings in the web address** (e.g., "amaz0n.com" instead of "amazon.com").
- **Poor grammar and unprofessional design.**
- **Too-good-to-be-true deals** (e.g., "Get a free iPhone!").
- **Strange pop-ups** asking for login details.

✅ **Always double-check the web address before clicking!**

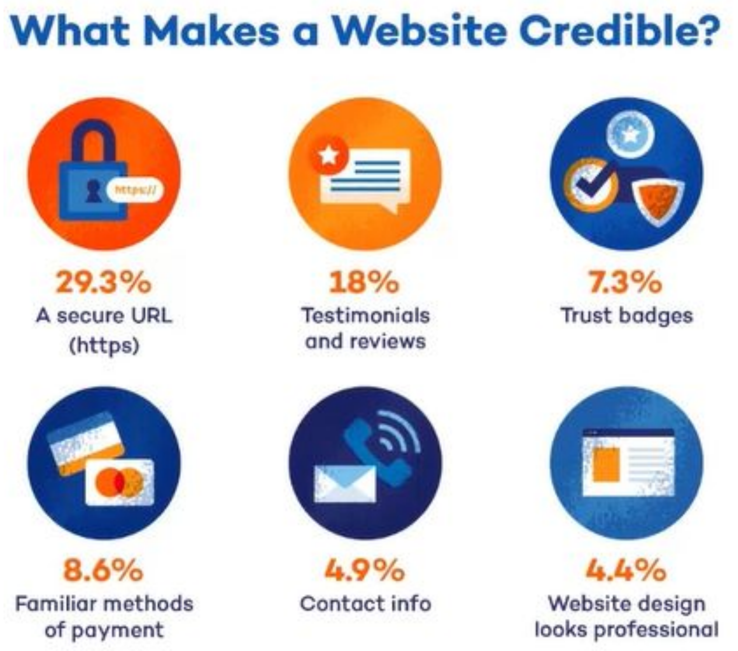
Security Warning!
SCAM
Danger! Virus detected
Close



# Understanding HTTPS vs HTTP

- → ✅ **Always check for HTTPS before entering personal details!**
- → **Secure ( 🔒 HTTPS) and an unsafe ( ⚠ HTTP). Still do NOT make payments even for HTTPS unless you totally trust the website!**

| Feature | HTTPS (Secure) | HTTP (Not Secure) |
|---|---|---|
| Encryption | Yes (protects data) | No (data can be stolen) |
| Padlock Icon | Yes 🔒 | No ❌ |
| Used by Trusted Sites | Yes | No |



## What Makes a Website Credible?

29.3%
A secure URL (https)

18%
Testimonials and reviews

7.3%
Trust badges

8.6%
Familiar methods of payment

4.9%
Contact info

4.4%
Website design looks professional

# Using Browser Security Warnings

🛑 If your browser says **"Not Secure" or "Deceptive Site Ahead"**:

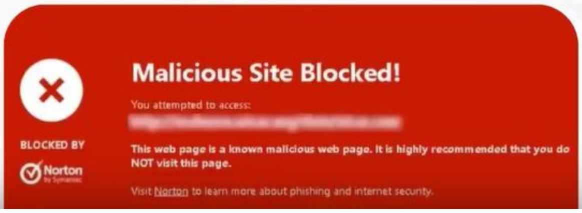
- Do NOT enter personal details.
- Close the tab immediately.
- Report the site if possible.

✅ **Update your browser** to stay protected from the latest threats!

# What to Do If You Visit an Unsafe Site

⚠️ **Steps to Take:**

1. **Close the site immediately.**
2. **Clear your browser history** (to remove tracking cookies).
3. **Run a security scan** if you accidentally downloaded something.
4. **Change passwords** if you entered login details.



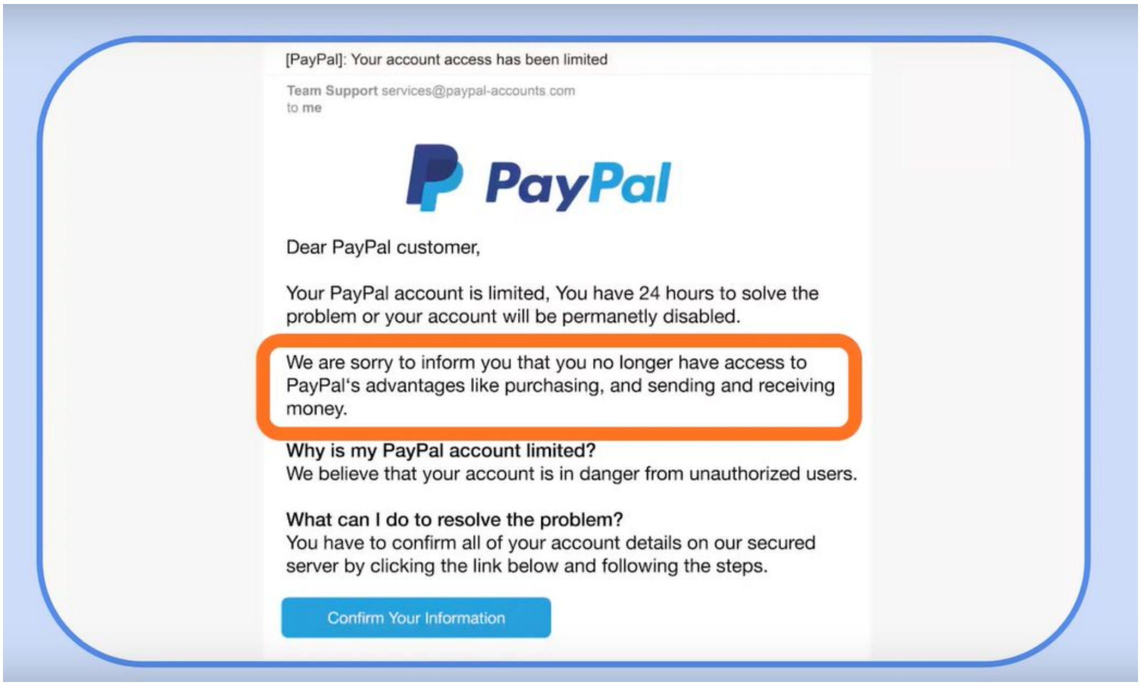
**Malicious Site Blocked!**

You attempted to access:

[redacted]

**This web page is a known malicious web page. It is highly recommended that you do NOT visit this page.**

Visit Norton to learn more about phishing and internet security.



[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to me

Dear PayPal customer,

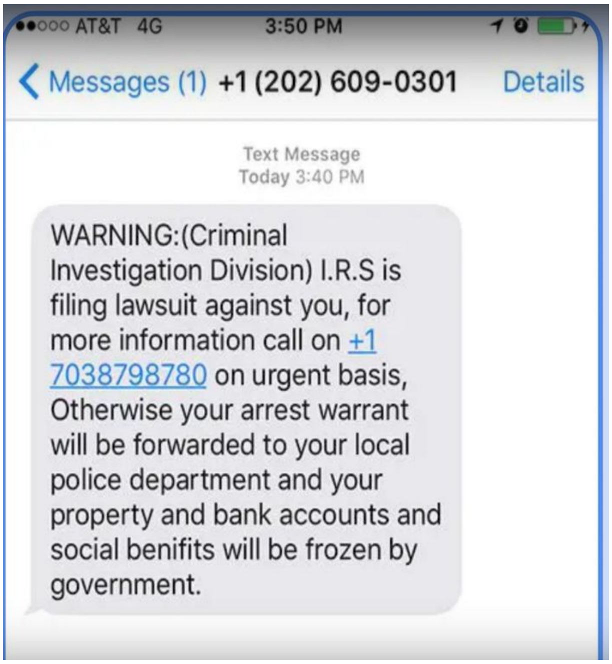
Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

**Why is my PayPal account limited?**
We believe that your account is in danger from unauthorized users.

**What can I do to resolve the problem?**
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

**Smishing (SMS Phishing)** messages are text message phishing attempts. Scammers send text messages pretending to be from reputable people, companies or authorities like the post office, IRS or police. They either direct you to a link or ask you to call a phone number.

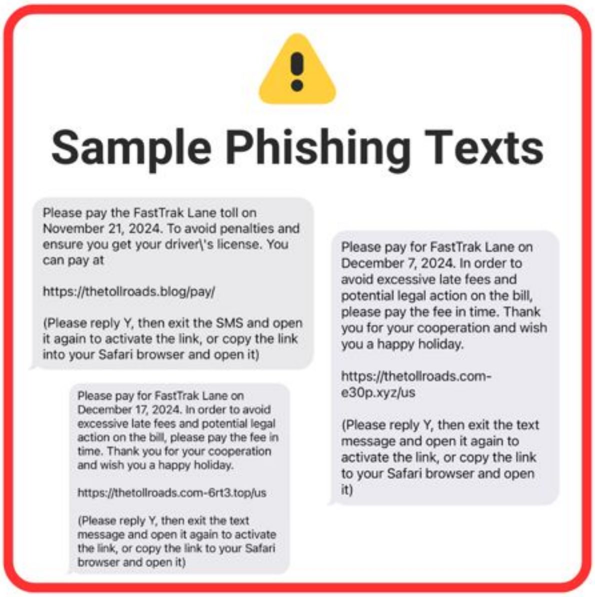


WARNING:(Criminal Investigation Division) I.R.S is filing lawsuit against you, for more information call on +1 7038798780 on urgent basis, Otherwise your arrest warrant will be forwarded to your local police department and your property and bank accounts and social benifits will be frozen by government.

OHIO
TURNPIKE

## Important Customer Advisory Regarding Nationwide Text Phishing Scam

https://www.ohioturnpike.org/



## Sample Phishing Texts

Please pay the FastTrak Lane toll on November 21, 2024. To avoid penalties and ensure you get your driver\'s license. You can pay at

https://thetollroads.blog/pay/

(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link into your Safari browser and open it)

Please pay for FastTrak Lane on December 17, 2024. In order to avoid excessive late fees and potential legal action on the bill, please pay the fee in time. Thank you for your cooperation and wish you a happy holiday.

https://thetollroads.com-6rt3.top/us

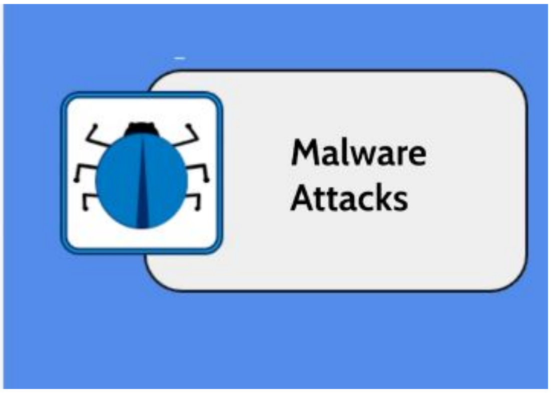
(Please reply Y, then exit the text message and open it again to activate the link, or copy the link to your Safari browser and open it)

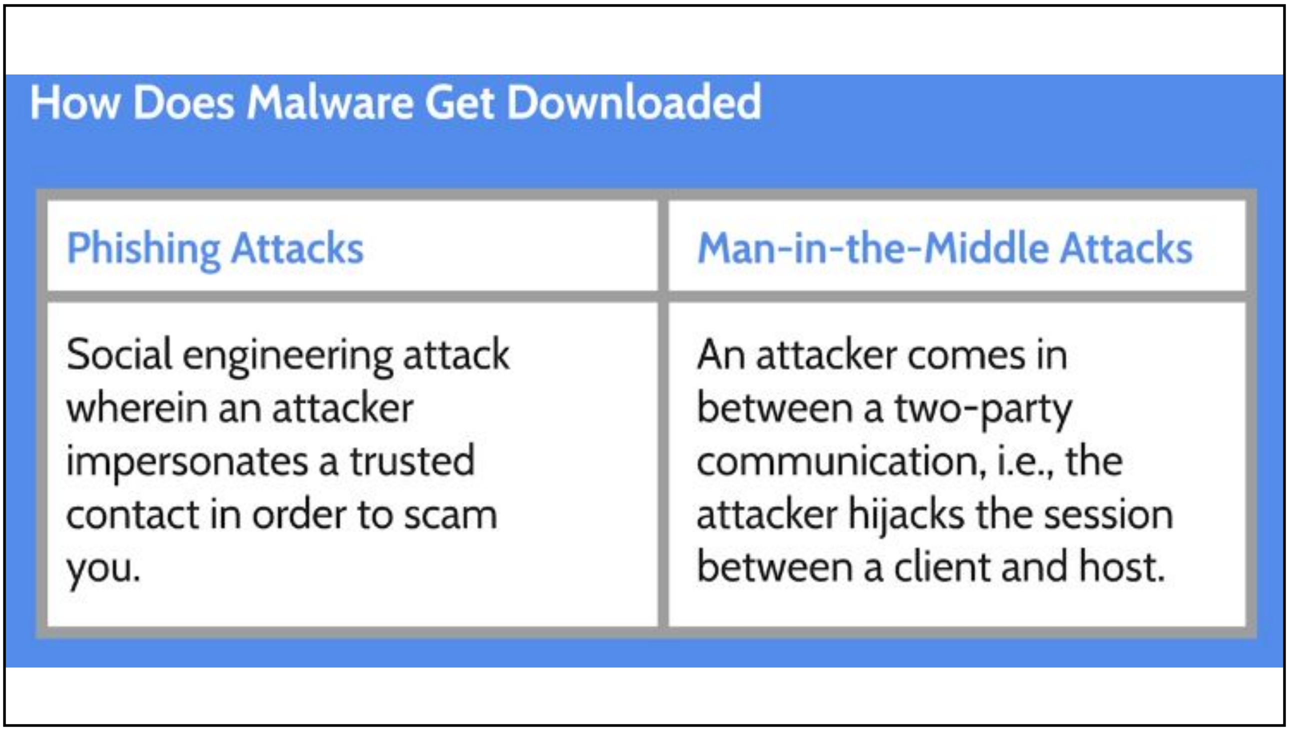
Please pay for FastTrak Lane on December 7, 2024. In order to avoid excessive late fees and potential legal action on the bill, please pay the fee in time. Thank you for your cooperation and wish you a happy holiday.

https://thetollroads.com-e30p.xyz/us

(Please reply Y, then exit the text message and open it again to activate the link, or copy the link to your Safari browser and open it)

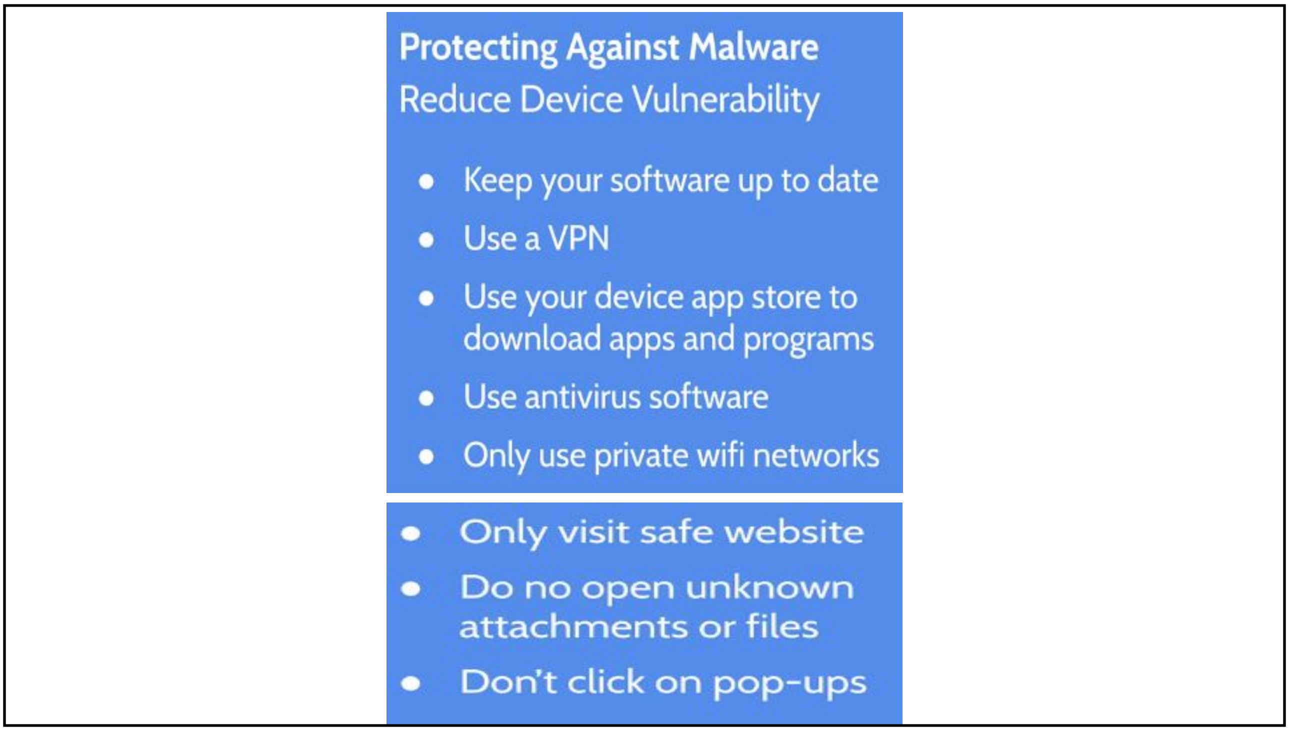
"**Malware**" refers to malicious software. This includes worms, spyware, ransomware, adware, and trojans.





## How Does Malware Get Downloaded

| Phishing Attacks | Man-in-the-Middle Attacks |
|---|---|
| Social engineering attack wherein an attacker impersonates a trusted contact in order to scam you. | An attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. |

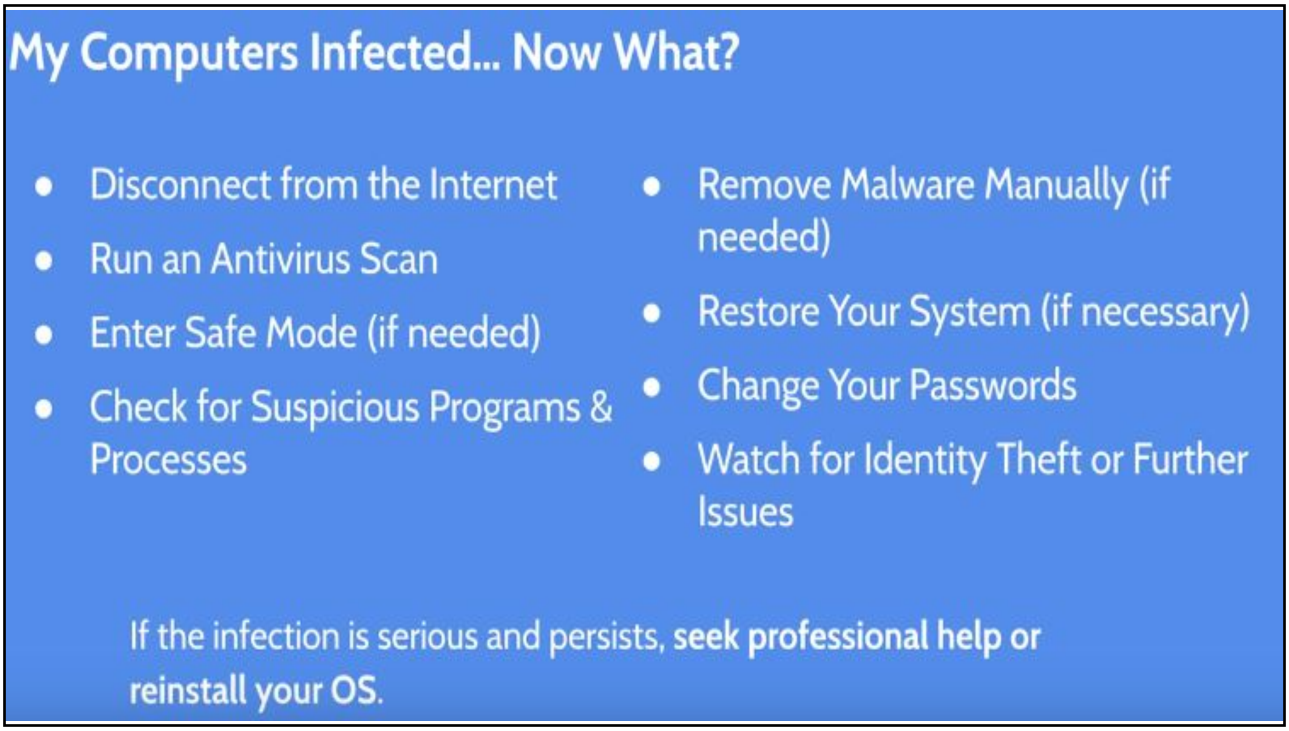


## Protecting Against Malware

### Reduce Device Vulnerability

- Keep your software up to date
- Use a VPN
- Use your device app store to download apps and programs
- Use antivirus software
- Only use private wifi networks

- Only visit safe website
- Do no open unknown attachments or files
- Don't click on pop-ups



## My Computers Infected... Now What?

- Disconnect from the Internet
- Run an Antivirus Scan
- Enter Safe Mode (if needed)
- Check for Suspicious Programs & Processes
- Remove Malware Manually (if needed)
- Restore Your System (if necessary)
- Change Your Passwords
- Watch for Identity Theft or Further Issues

If the infection is serious and persists, **seek professional help or reinstall your OS.**

**Download my online course, lecture, & PDF.**
Online ads and commercials offering any easy way to learn a skill for cheap. It will always lead to more things to buy or is inadequate material.

**Survey / Watch TV / Phone Game scam**
Easy way to obtain your info for next promising the user money or gift cards.

# The different types of scams in depth

EMPLOYMENT
SCAM

CHARITY
SCAM

PHONE
SCAM

**Grandparent Scams:**

Scammers pose as a child or grandchild in trouble, requesting money or gift cards.

**Romance Scams:**

Con artists pretend to be romantic partners on dating sites or social media to gain trust and then request money.

**Tech Support Scams:**

Scammers claim to offer computer assistance, gaining remote access to devices and personal information.

**Medicare Impersonation:**

Scammers pretend to be Medicare representatives, requesting personal information or offering fake services for reimbursement.

**Investment Scams:**

Fraudsters offer fraudulent investment opportunities, often involving cryptocurrency, to lure seniors into investing.

**Sweepstakes/Lottery Scams:**

Scammers claim a senior has won a prize and request fees or personal information to release it.

**Charity Scams:**

Scammers pretend to represent charities to solicit donations.

**Government Impersonation Scams:**

Scammers impersonate government officials (IRS, Social Security) to scare seniors into providing information or money.

**Telemarketing Scams:**

Scammers use telemarketing to sell fake products, offer fraudulent investments, or request donations.

## How do I protect myself from scammers?

Here are some ways to protect yourself:

◁ **Don’t respond** to unexpected calls, emails, texts, or social media messages that ask for money or personal information.

◁ **Take your time.** Honest organizations will give you time to make a decision. Anyone who pressures you to pay or give them your information is a scammer.

◁ **Never pay** someone who insists you can only pay with a gift card, a wire transfer, cryptocurrency, or a payment app.

## Protect Yourself and Your Information

- Don’t carry your important papers or ID cards with you.
- Don’t click on links in emails, texts, or social media messages unless you’re sure you know what they are.
- Don’t trust caller ID. Scammers can make any name or number show up on your caller ID.
- Don’t send money to anyone who calls, emails, or texts and says they’re with the government.
- A government seal doesn’t mean a website is official. Look for **.gov** in the address.
- Never pay for immigration forms from the U.S. government. They are free.
- If you think someone stole your identity, visit **IdentityTheft.gov** for help.

**Freeze your social security number**

**Tips for Staying Safe:**

- **Verify the identity of anyone contacting you, especially if they are asking for money or personal information.**
-
- **Be wary of offers that seem too good to be true, or if you are pressured to act immediately.**
-
- **Never click on links in unsolicited emails or text messages.**
-
- **Don't send money to someone you've never met in person.**
-
- **Be skeptical of anyone who claims to represent a government agency and demands immediate payment or action.**
-
- **Report suspected scams to the Federal Trade Commission (FTC) at ReportFraud.ftc.gov.**
-
- **Consider signing up for the Do Not Call Registry to reduce telemarketing calls.**

## If I sent money to a scammer, what should I do?

If you paid or sent money to someone you think is a scammer, you might not get it back.
But it’s always worth asking the company you used to send the money if there’s a way to get it back.

Try to cancel or reverse the transaction as soon as you can.

**1.Contact whoever you used to send money, for example:**

◃ Credit card company or bank

◃ Money transfer company (like Western Union or MoneyGram)

◃ Gift card company

◃ Cryptocurrency company

◃ Post office

**2. Tell them it was a scam**

**3. Ask them to give your money back If you gave cash or gold to someone, call the police.**

https://www.youtube.com/@cyberseniorscorner/videos

https://cyberseniors.org/cybersecurity