What Should You Do After Falling Victim to an Online Scam

Online scams can be devastating, especially for those over 50. In this presentation, we'll share simple steps on what to do after falling victim to an online scam.

Understanding Online Scams

Online scams are fraudulent schemes that trick individuals into giving away their personal or financial information. They can range from phishing scams that attempt to obtain passwords or credit card numbers to lottery scams that promise large payouts in return for small fees. Learning to identify these scams is critical in avoiding becoming their next victim.

Phishing Scams

A scammer sends an email or text message pretending to be a legitimate institution to trick you into giving your personal information.

Lottery Scams

Scammers claim you've won a large sum of money and require you to pay a small fee to receive the payout.

Signs of Having Been Scammed

It's essential to recognize if you've fallen victim to an online scam.
Here are some common signs:

1 Urgent Requests

Scammers demand immediate action, such as clicking on a link or providing personal information.

2 Unsolicited Messages

You receive a message from someone or an institution you didn't contact or expect to hear from.

3 Requiring Payment in Gift Card

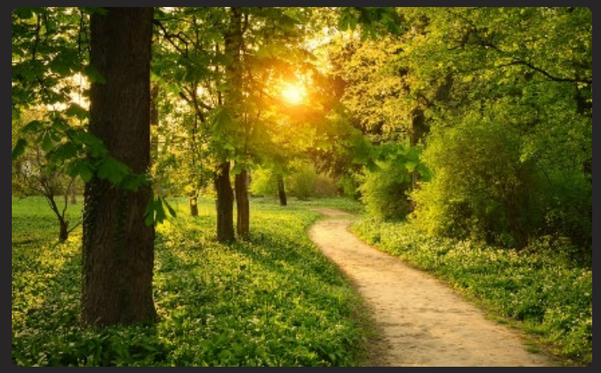
Scammers will often ask you to buy a gift card

Stay Calm and Take a Breath

If you realize you fell for a scam, take a deep breath and remain calm. Avoid panicking and making hasty decisions.

Meditate

Take 10 minutes to meditate and clear your mind of anxiety.



Take a Walk

Walk in nature to refresh your mind and gain some clarity.

Relax with Tea

Sipping a cup of hot tea can help calm your nerves and destress.

Disconnect and Report

The moment you realize you've fallen for a scam, disconnect from the platform immediately and contact website administrators to report the incident.

Disconnect ASAP

Close the window or exit the app immediately.

Contact Website Administrators

Report the incident to the website or platform administrators.

Contact Your Bank or Credit Card Company

After reporting the scam, contact your financial institution for assistance in possibly stopping or reversing any fraudulent activity.

Call Your Bank or Credit Card Company

Call the phone number on the back of your bank or credit card for assistance.

1

Gather Account Information

Gather all your account information before calling.

2

3

Provide Details

Provide the details of the scam and any fraudulent activity in your account.

Seek Professional Help

Don’t hesitate to seek help from a tech-savvy friend or a reputable authority to assist in tech-related issues.

Friends and Family

Reach out to tech-savvy friends or family members for help in resolving any issues or vulnerabilities.

Find a Professional

Always have a reliable professional on call

Change Passwords & Enable 2 Factor Authentication (2FA)

Scammers may have obtained your passwords. Change your passwords for all affected accounts as soon as possible.

How to Change Passwords

Log in to your accounts and find the password change option, typically located in the security settings.

Password Management Tips

- Use strong passwords and avoid using the same password for multiple accounts.
- Consider using password management tools such as LastPass or 1Password.

Enable 2 Factor Authentication (2FA)

Two-factor authentication (2FA) is a security system that requires two forms of identification to access your account. The first factor is a password, and the second factor is usually a security code sent to your phone or email.

Educate Yourself

Arm yourself against future scams by learning to identify them. Stay informed of the latest scams through trusted sources and websites.

1 Trusted Websites

- Federal Trade Commission: www.ftc.gov
- AARP Scams: www.aarp.org/money/scams-fraud/

2 Latest Scams

- Fraud!org: https://fraud.org/
- FBI: https://www.fbi.gov/common-scams-and-crimes

Be Cautious with Personal Information

Check Sender's Email

Double-check the email address and domain name of the sender.

Verify Requests

If a request seems suspicious, verify it by calling the organization directly.

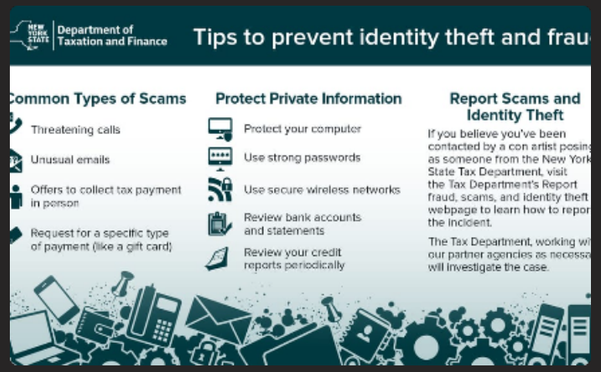
Limit Personal Info

Be mindful of sharing your sensitive information, even postal address.

Protect Payment Details

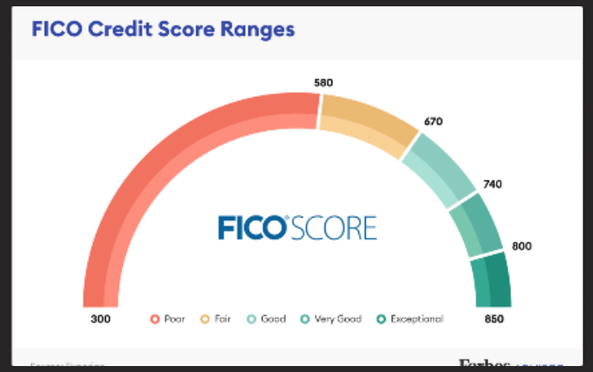
Never disclose your financial details, use trusted payment options only.

Reclaiming Your Identity



File a Report

Report the scam to the relevant authorities immediately.



Fraud Alert

Place a fraud alert on your credit report to prevent further damage.

Identity Protection

Consider opting for an identity protection service to monitor your accounts.

Learn from the Experience

1

Stay Informed

Use your experience to keep up-to-date with the latest scams and online tricks.

2

Share with Family & Friends

Spread awareness of common scams to your loved ones.

3

Report Scams

Report any unusual activities or scams to the FTC or BBB so they can alert the public.

Stay Informed

Subscribing for Newsletters

Subscribe to newsletters or alerts from trusted sources to stay informed and up-to-date with the latest scams.

Connect with Professionals

Join forums or groups where professionals share share experience about scams and provide solutions to overcoming overcoming them.

Spread Awareness

Host a Community Workshop

Host workshops to educate your community about how to identify and avoid scams.

Talk to Your Family

Start conversations with your family and loved ones about online risks and how to protect themselves.

Be Active on Social Media

Use social media platforms to your advantage and raise awareness about online scams with a wider audience.

Resources

Websites:

ftc.gov
fbi.gov
ic3.gov

Hotlines:

FTC Hotline:
1-877-FTC-HELP
(1-877-382-4357)
BBB Hotline:
1-888-670-9888

Community Groups:

Facebook groups like
Scam Watch or
Fraud Alert.

Recap

1 Report Scams

Report all scams to relevant authorities as quickly as possible.

2 Stay Informed

Subscribe to alerts and newsletters to stay aware of the latest scams.

3 Protect Your Identity

Take action to protect your identity thoroughly after a suspected scam.

4 Spread Awareness

Talk to family, host workshops, and be active on social media to spread awareness and prevent others from falling victim to scams.

5 Stay Safe

Stay diligent and protect your personal information at all times to stay safe online.