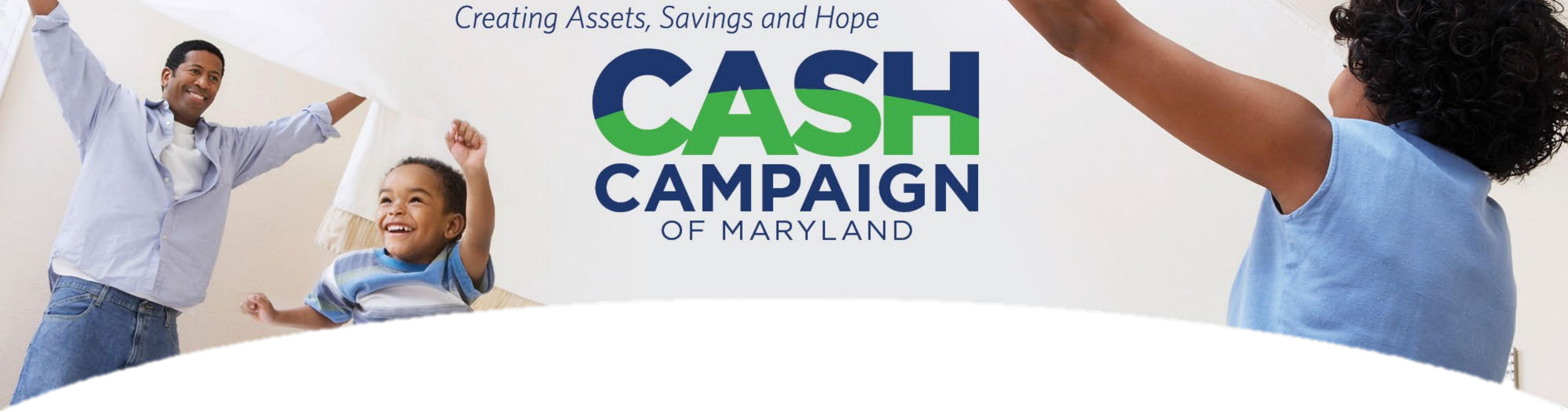
Creating Assets, Savings and Hope

CASH CAMPAIGN
OF MARYLAND

Cybersecurity and Scams 101

Updated July 2024



Creating Assets, Savings and Hope

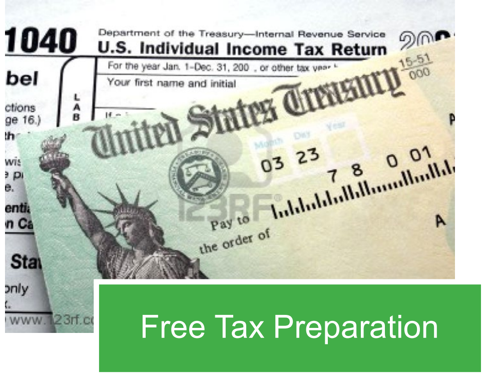
CASH CAMPAIGN OF MARYLAND

The CASH (Creating Assets, Savings and Hope) Campaign of Maryland promotes economic advancement for low-to-moderate income individuals and families in Baltimore and across Maryland.

Creating Assets, Savings and Hope

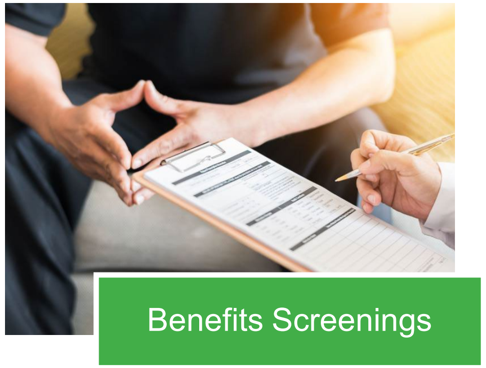
CASH CAMPAIGN OF MARYLAND

What We Offer:



Free Tax Preparation

Financial Education Workshops/Conferences

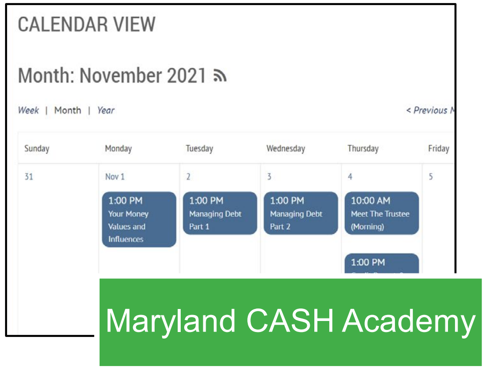


Benefits Screenings

Unknown Author is licens

Financial Coaching

Financial Fitness Fairs



CALENDAR VIEW

Month: November 2021

Week | Month | Year

< Previous

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday
31	Nov 1 1:00 PM Your Money Values and Influences	2 1:00 PM Managing Debt Part 1	3 1:00 PM Managing Debt Part 2	4 10:00 AM Meet The Trustee (Morning) 1:00 PM	5

Maryland CASH Academy

Advocacy and Policy

Bank On Maryland

www.cashmd.org/

www.mdcashacademy.org/

www.bankonmaryland.org/

Creating Assets, Savings and Hope

Objectives

Understand

- The statistics and trends of consumer scams today

Discover

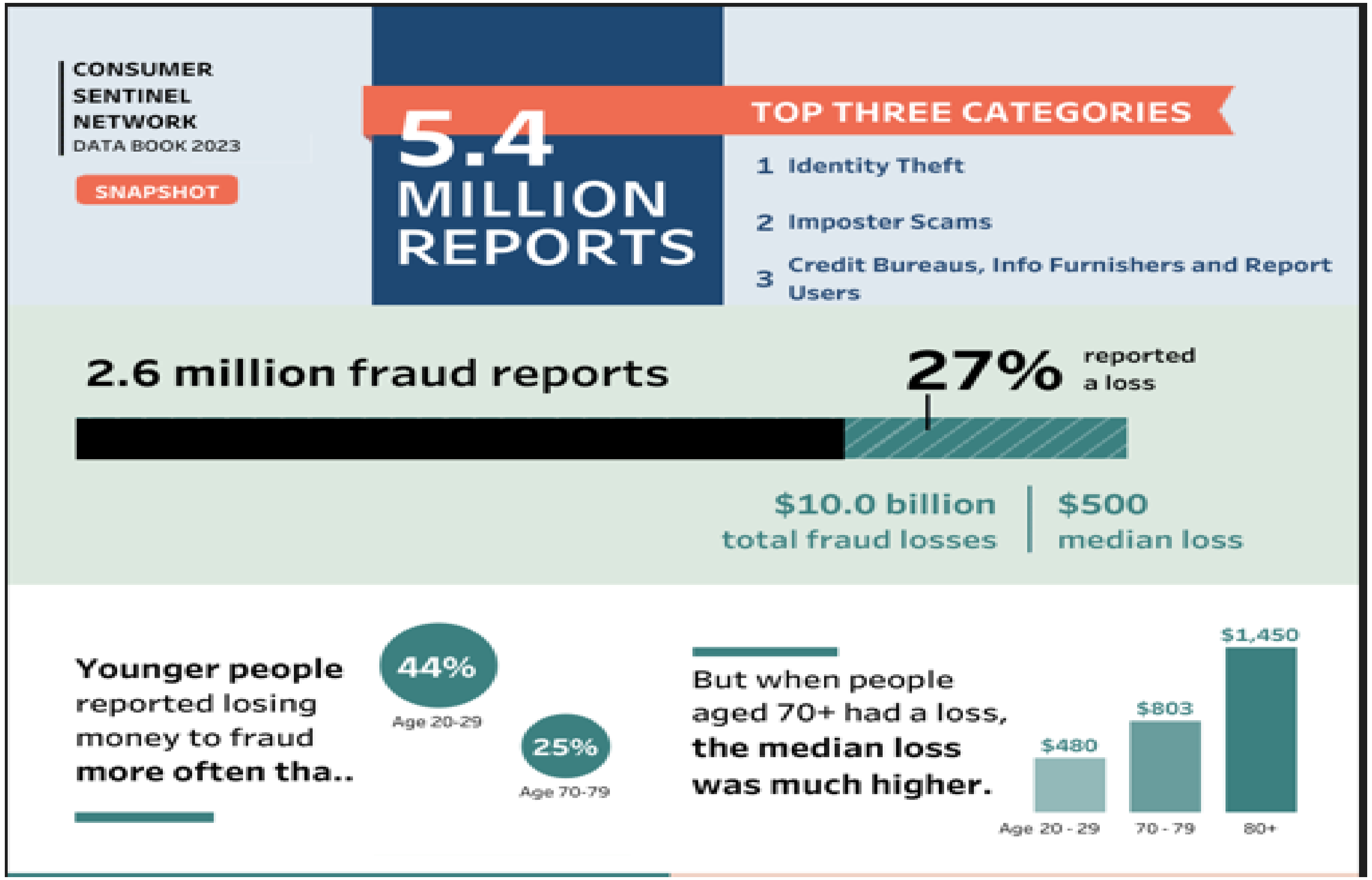
- What makes people and machines vulnerable to scams and cyber attacks
- How to protect your information online

Learn

- What are the leading agencies that are protecting consumers
- What steps to take if you are a victim of scams or fraud and where to report

Consumer Financial Fraud

This occurs when a person suffers from a financial loss involving the use of deceptive, misleading, or other illegal practices.



CONSUMER SENTINEL NETWORK DATA BOOK 2023

SNAPSHOT

5.4 MILLION REPORTS

TOP THREE CATEGORIES

1 Identity Theft

2 Imposter Scams

3 Credit Bureaus, Info Furnishers and Report Users

2.6 million fraud reports

27% reported a loss

$10.0 billion total fraud losses

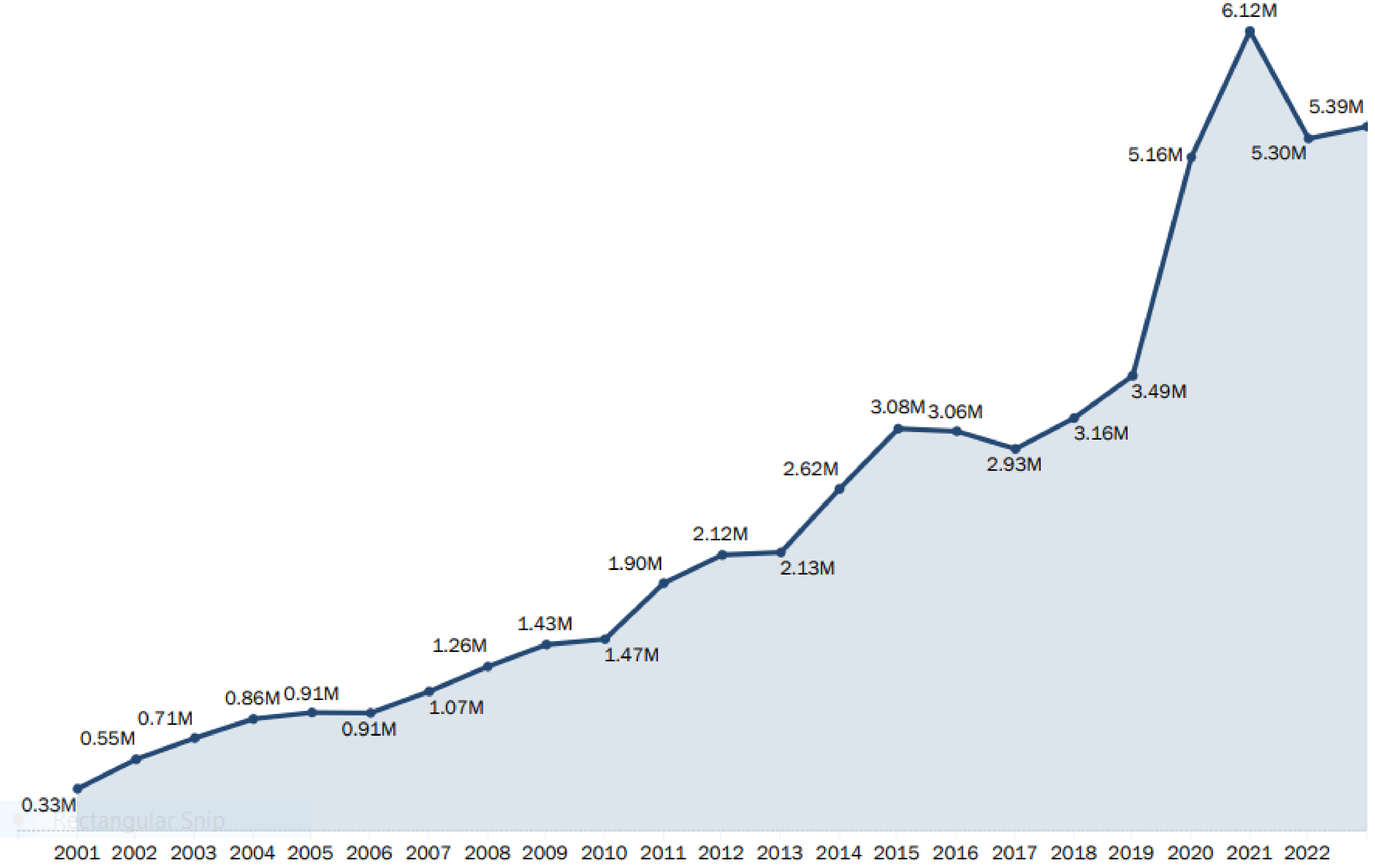
$500 median loss

Younger people reported losing money to fraud more often tha..

But when people aged 70+ had a loss, the median loss was much higher.

Number of Fraud, Identity Theft and Other Reports by Year

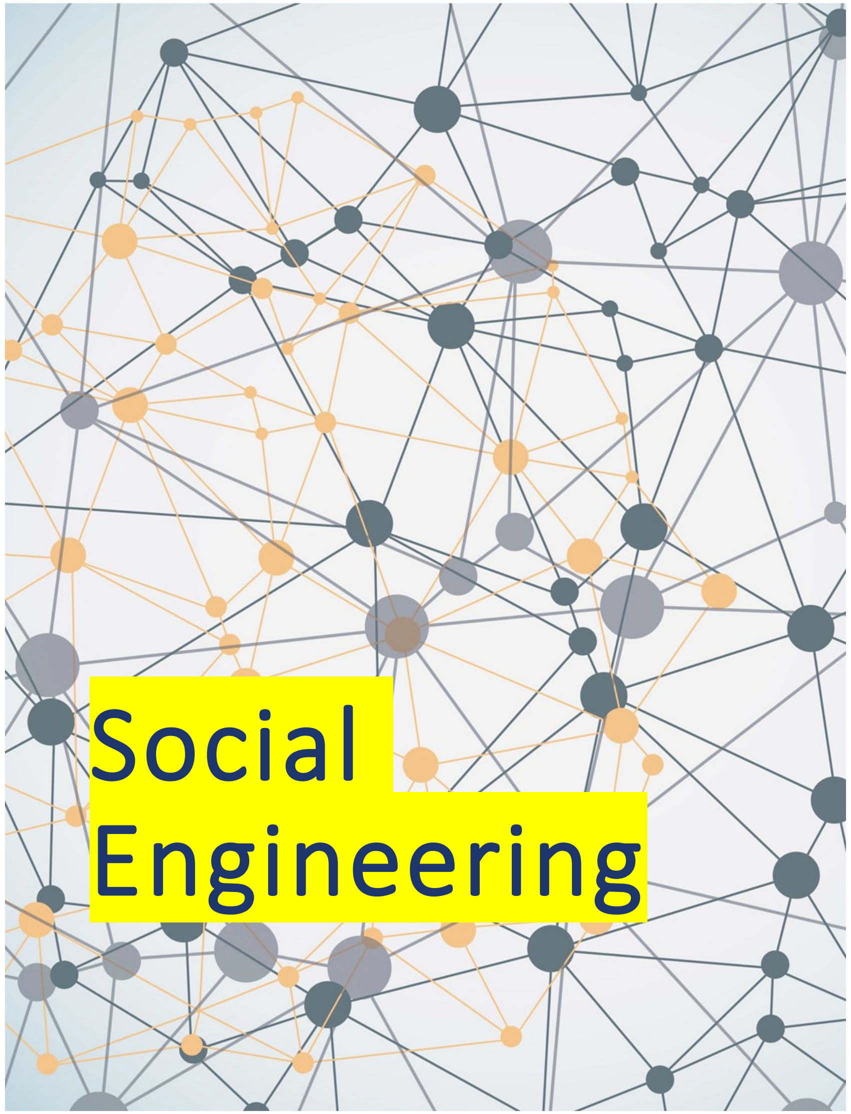
CASH CAMPAIGN OF MARYLAND



Creating Assets, Savings and Hope

Environmental and Emotional Factors

- Stressful life events
- Less Social/Family Support
- Stronger Emotions
- Targeted by Scammers



Social Engineering

“Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information.

It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.”

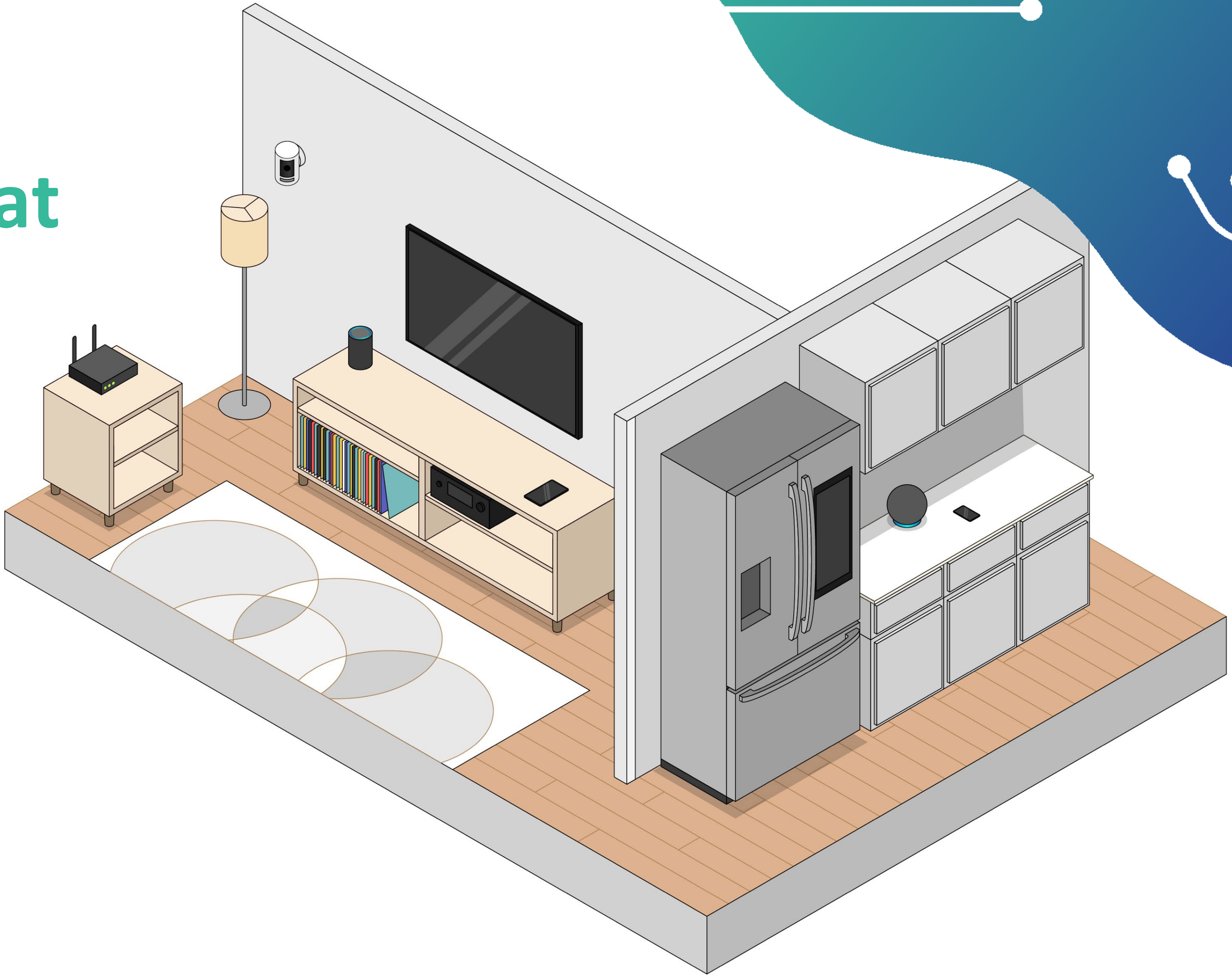
Elements of Social Engineering Attacks

- **Pretext – The lie they tell**
- **The Appeal – Eliciting a strong emotion to prompt action**
- **Artificial time constraint**
- **The call to action**
- **Isolation**

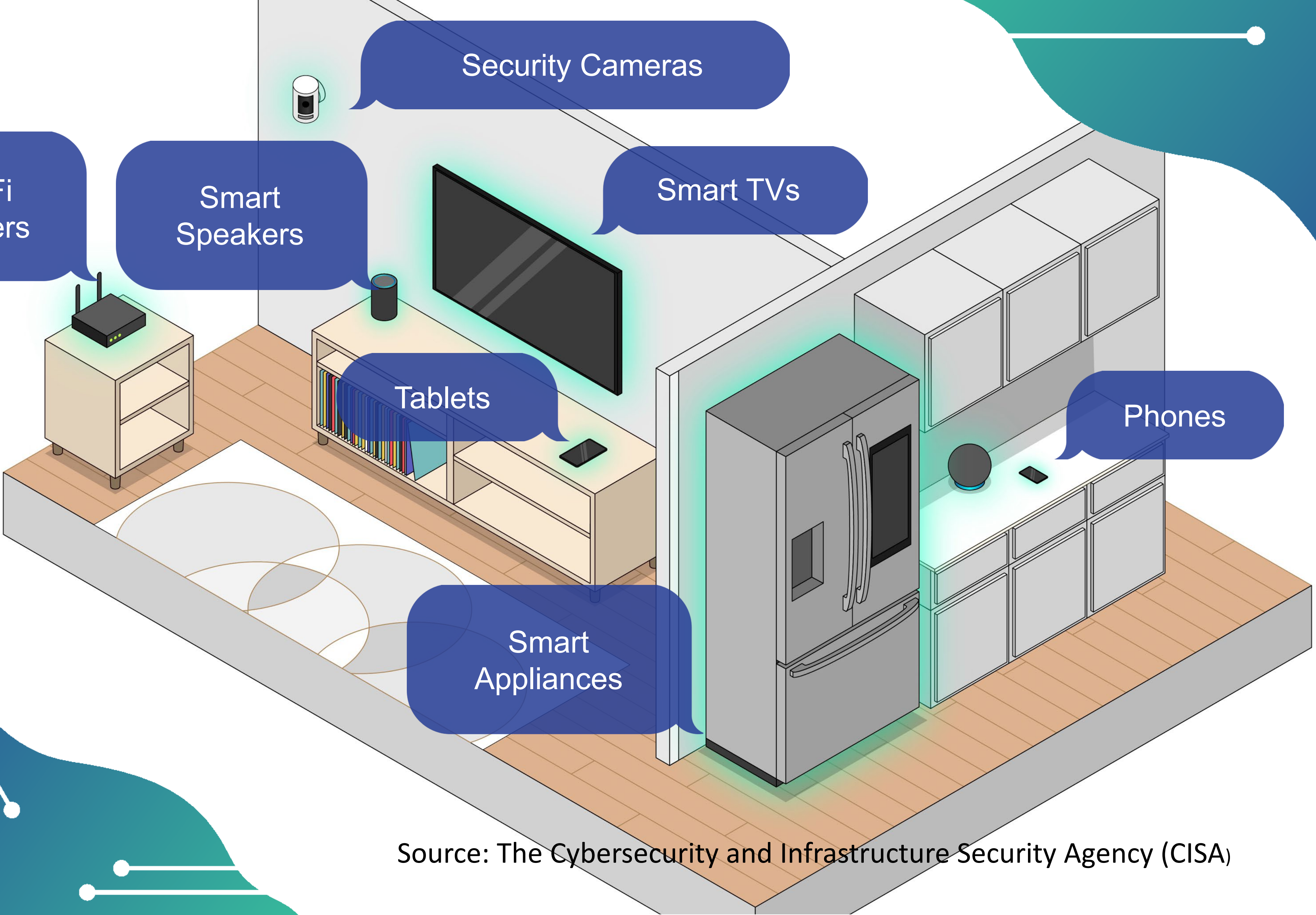
Source: John Hopkins Presentation The Bad Guys and You: Understanding Your Risk Model

Identify Potential Cyber Risks – What can be Hacked?

- Look at this house to see what devices you can identify that may pose a cybersecurity risk.
- Write down everything you find, what makes it a risk and ways you could alleviate that risk.



Source: The Cybersecurity and Infrastructure Security Agency (CISA)



Source: The Cybersecurity and Infrastructure Security Agency (CISA)

Phishing, Vishing, and Smishing – Oh My!

Phishing Attack

- use email or malicious websites
- solicit personal information
- pose as a trustworthy organization
- Take advantage of current events and certain times of year
- Shortened URLs, incorrect email addresses or links “amaz**a**n.com”
- Occasional Poor grammar/misspellings

Vishing Attack

- voice communication
- entices a victim to call a certain number and divulge sensitive information.
- Voice over Internet Protocol (VoIP) easily allows caller identity (ID) to be spoofed

Smishing Attack

- SMS, or text, messages
- Can contain links to webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number.

A I Voice Cloning?

Signs:
You are contacted out of the blue.
You are pressured to act immediately, with no time to think.
The caller is urgently requesting money, usually through a wire transfer, gift card, payment app, or cryptocurrency.
The caller is requesting personal or private information from you.
You are told to keep the caller’s request a secret.

What to do:
Use a family code word
Don't Panic
Call the family member directly

Information Security Breeches

Photo Illustration: matejmo/Getty Images

Protect Yourself Against Social Engineering Attacks

Discuss things with trusted friends.

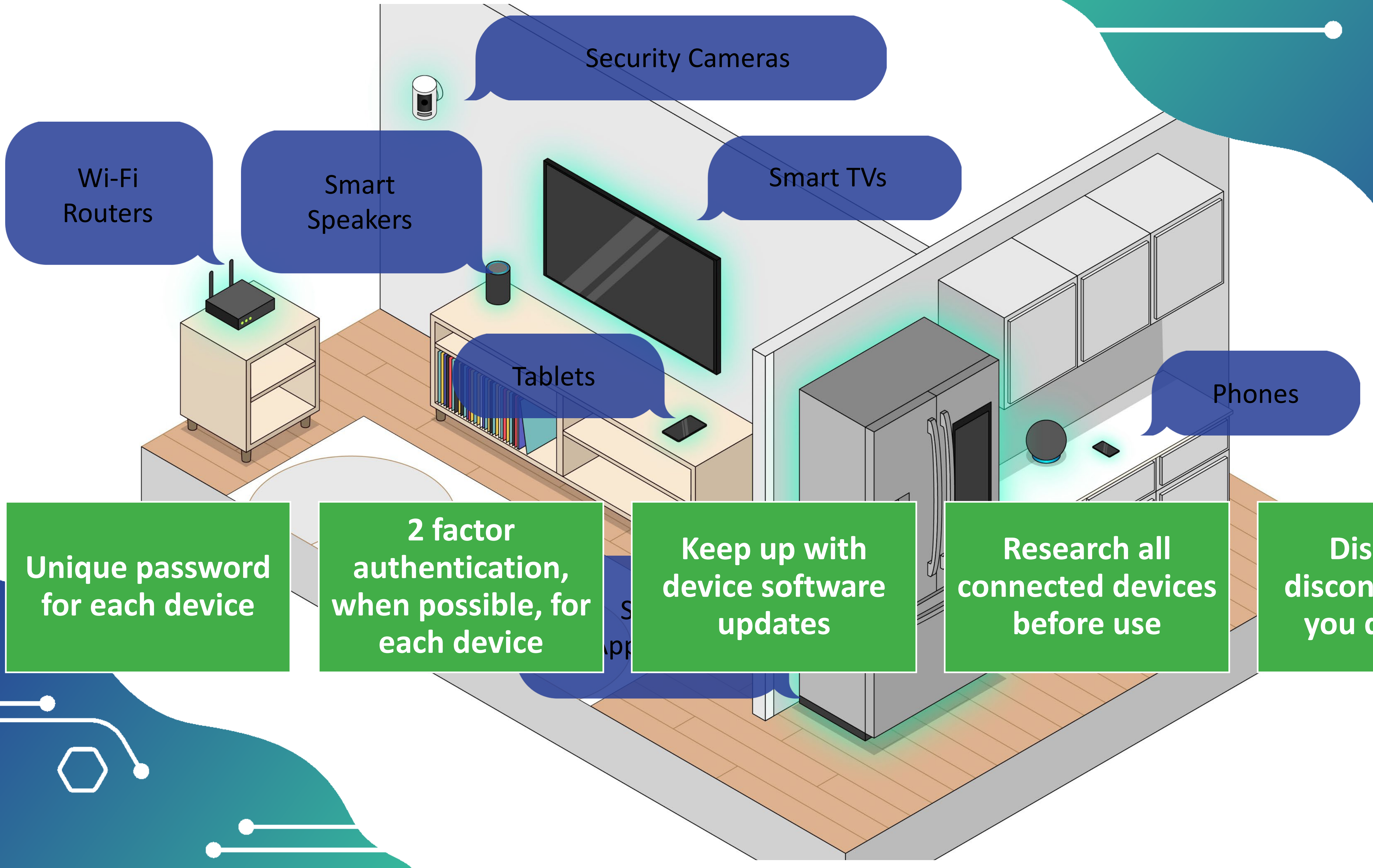
Don’t give out information or act on inbound calls

Learn and know the patterns - “red flags”

Source: John Hopkins Presentation The Bad Guys and You: Understanding Your Risk Model

Cybersecurity Hygiene

- Use strong passwords, and ideally a password manager to generate and store unique passwords
- Implement multi-factor authentication (MFA)
- Update your software. Turn on automatic updates.
- Think before you click. More than 90% of cyber-attacks start with a phishing email.
- Share with care. Think before posting



Unique password for each device

2 factor authentication, when possible, for each device

Keep up with device software updates

Research all connected devices before use

Disable or disconnect what you don't use

Information/Security Breeches

The Maryland Personal Information Protection Act (PIPA)

- Went into effect in January 2008.
- Requires any business that keeps electronic records containing the personal identifying information (PPI) of Maryland residents to notify those residents if their information is compromised.
- Records of security breeches for the last three years can be found on the MD Attorney General's website https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx

ID Theft – Next Steps

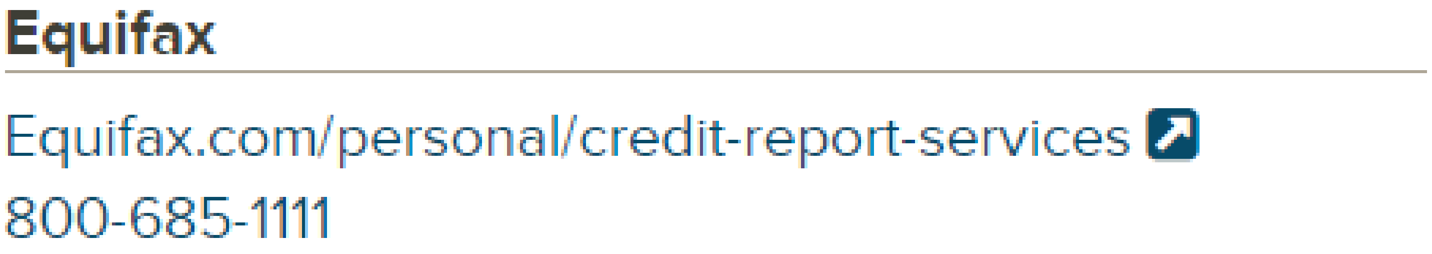
- Police Report – Non- emergency number
- Check credit reports – Annualcreditreport.com
- Fraud Alert
- Freeze on Credit
- Contact Credit Card Company/Bank
- New Passwords
- File with Consumer Protection/FTC

Fraud Alerts & Credit Freezes:
What's the Difference?

Looking for ways to protect your identity?
Here are two options to consider.

Fraud Alert	Credit Freeze
✓ Makes lenders verify your identity before granting new credit in your name. (Usually, they'll call you to verify your identity.)	✓ Restricts access to your credit report to help prevent identity theft. (Usually, you'll need a PIN or password to place or lift the freeze.)
✓ Free	✓ Free
✓ Available to anyone who is or suspects they may be affected by identity theft	✓ Available to anyone
✓ Lasts one year	✓ Lasts until you lift it
✓ To place: Contact **one** of the three credit bureaus. That bureau must tell the other two.	✓ To place or lift: Contact **all three** credit bureaus. (If you know which bureau a lender will use, you can lift for only that one.)

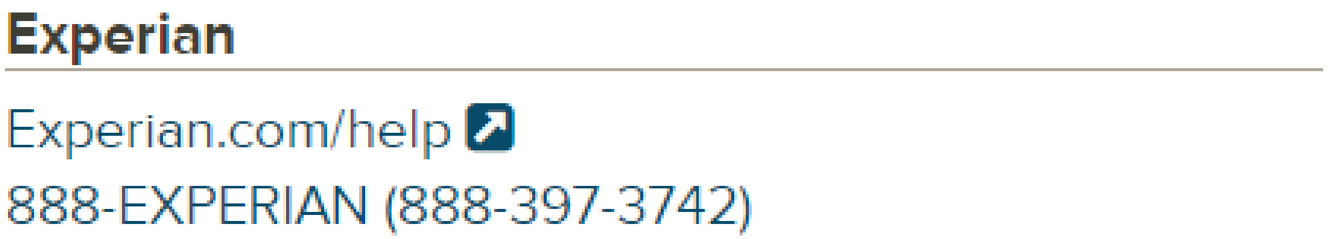
Credit Bureau Contacts



Equifax

Equifax.com/personal/credit-report-services

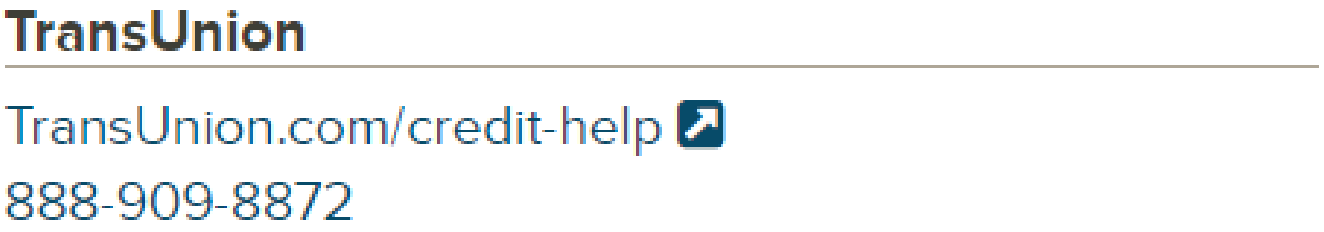
800-685-1111



Experian

Experian.com/help

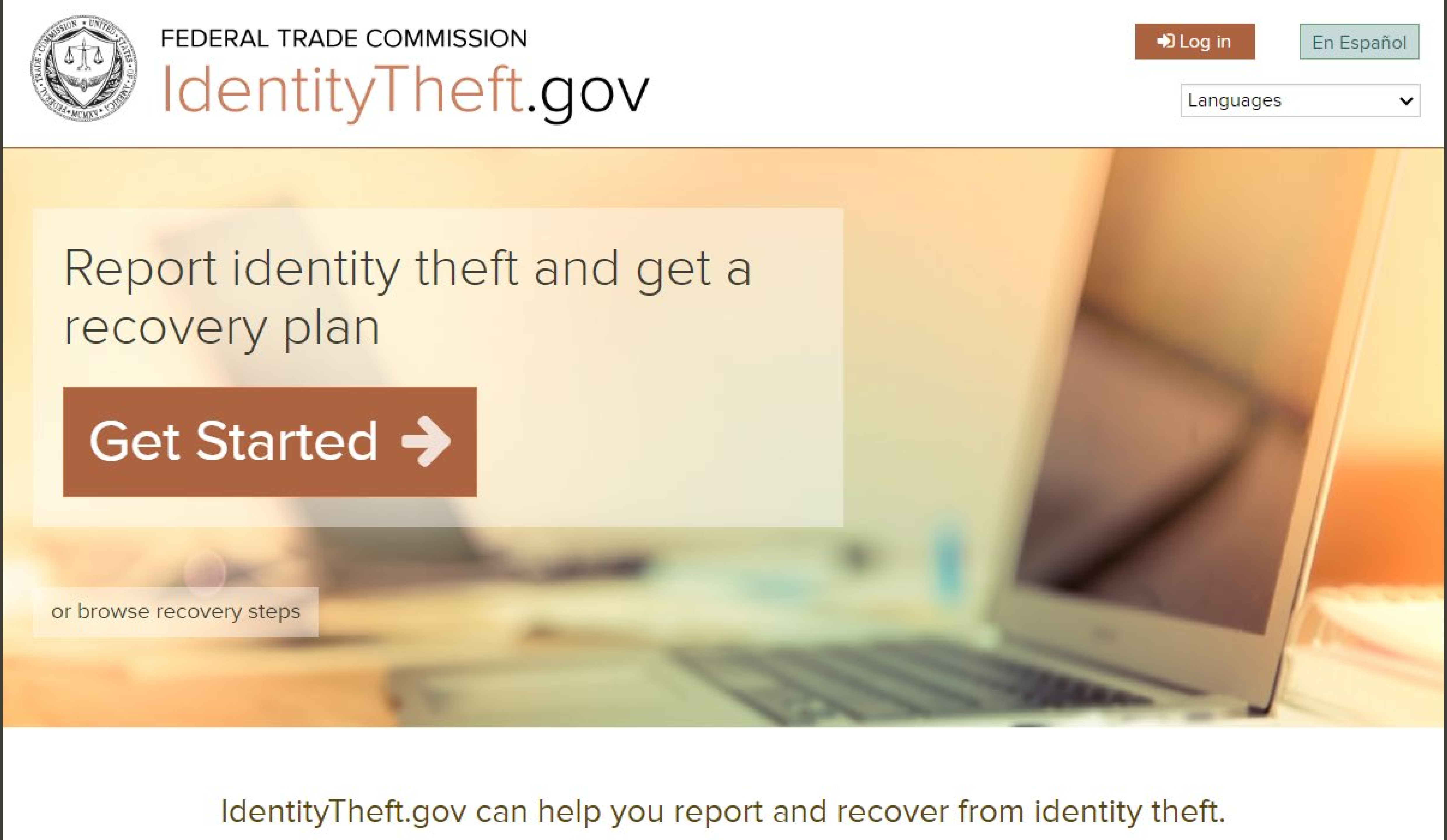
888-EXPERIAN (888-397-3742)



TransUnion

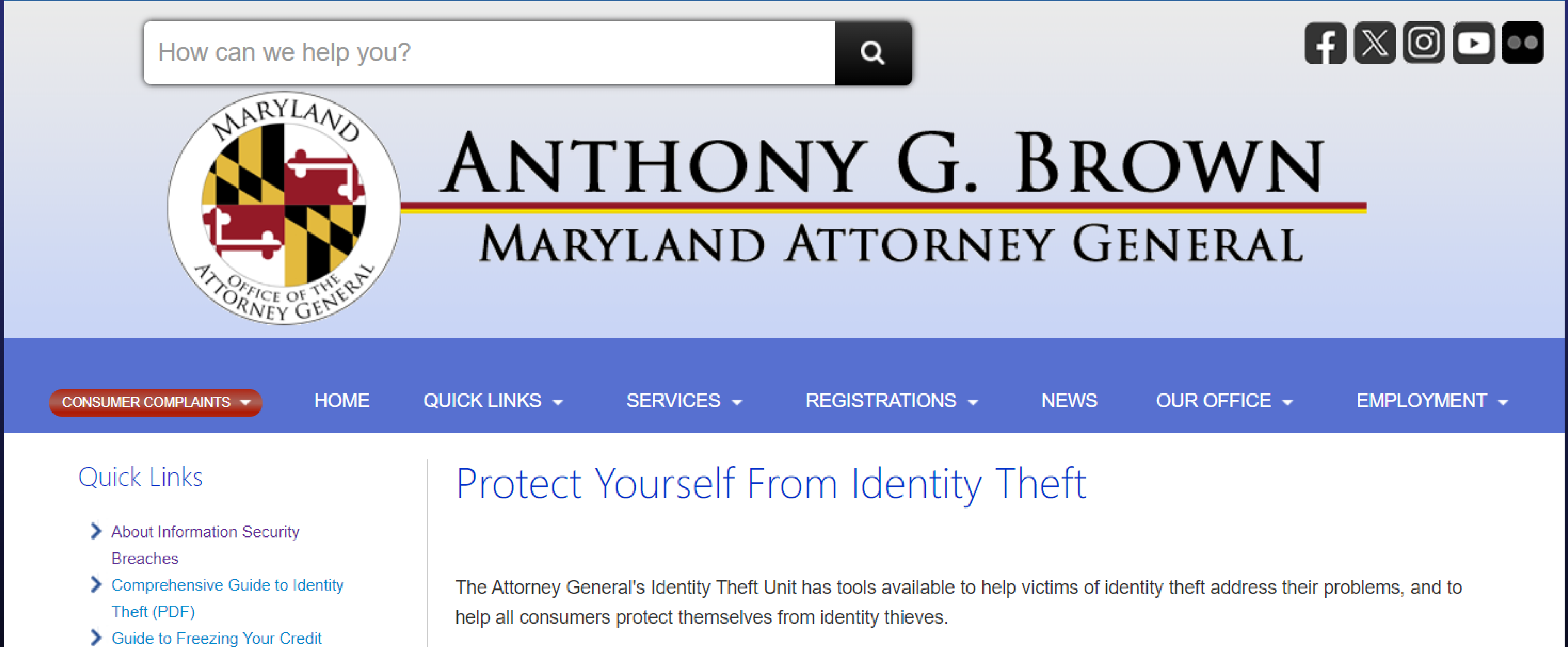
TransUnion.com/credit-help

888-909-8872



Report identity theft and get a recovery plan

IdentityTheft.gov can help you report and recover from identity theft.



Quick Links

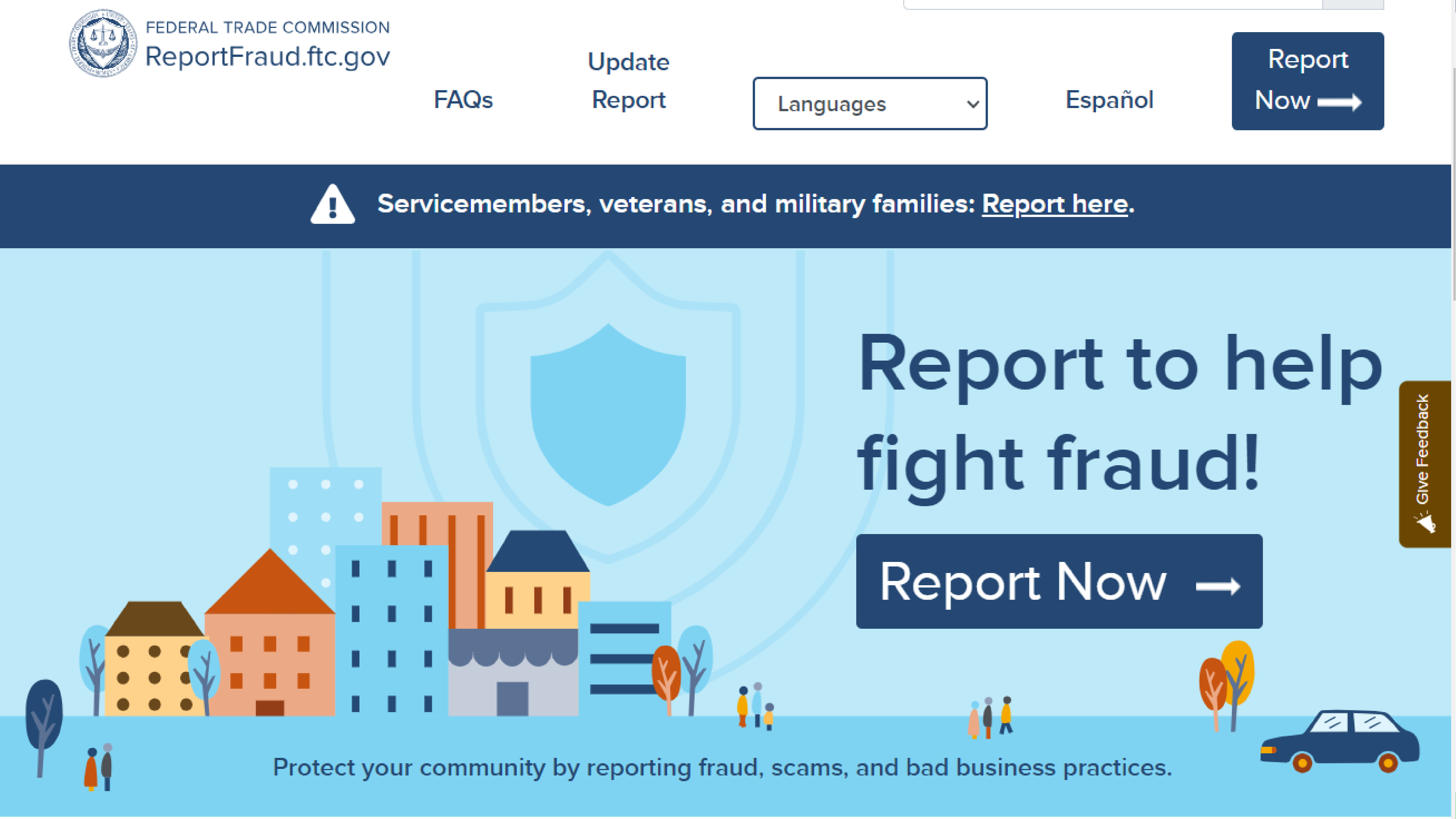
- About Information Security Breaches
- Comprehensive Guide to Identity Theft (PDF)
- Guide to Freezing Your Credit

Protect Yourself From Identity Theft

The Attorney General's Identity Theft Unit has tools available to help victims of identity theft address their problems, and to help all consumers protect themselves from identity thieves.

Contact the Identity Theft Unit

Phone: (410) 576-6491 Fax: (410) 576-6566 Email: idtheft@oag.state.md.us

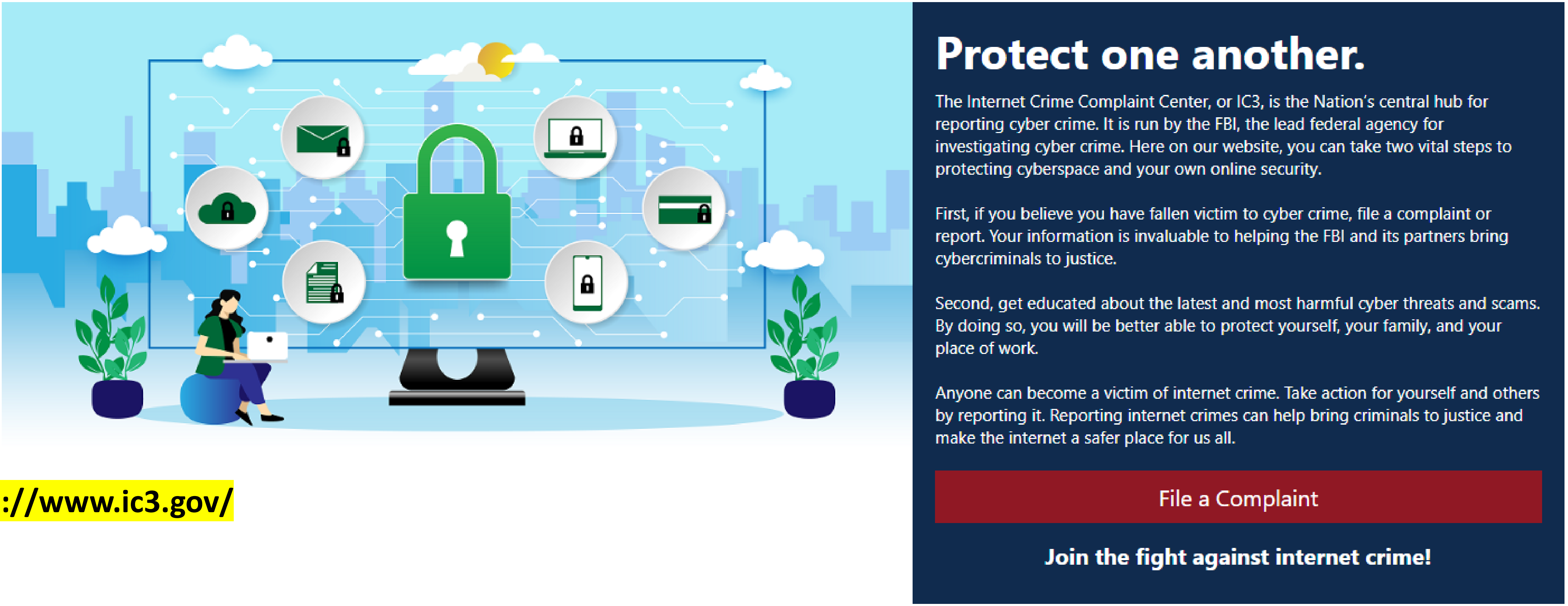


Servicemembers, veterans, and military families: Report here.

Report to help fight fraud!

Protect your community by reporting fraud, scams, and bad business practices.

Internet Crime Complaint Center (IC3)



Protect one another.

The Internet Crime Complaint Center, or IC3, is the Nation's central hub for reporting cyber crime. It is run by the FBI, the lead federal agency for investigating cyber crime. Here on our website, you can take two vital steps to protecting cyberspace and your own online security.

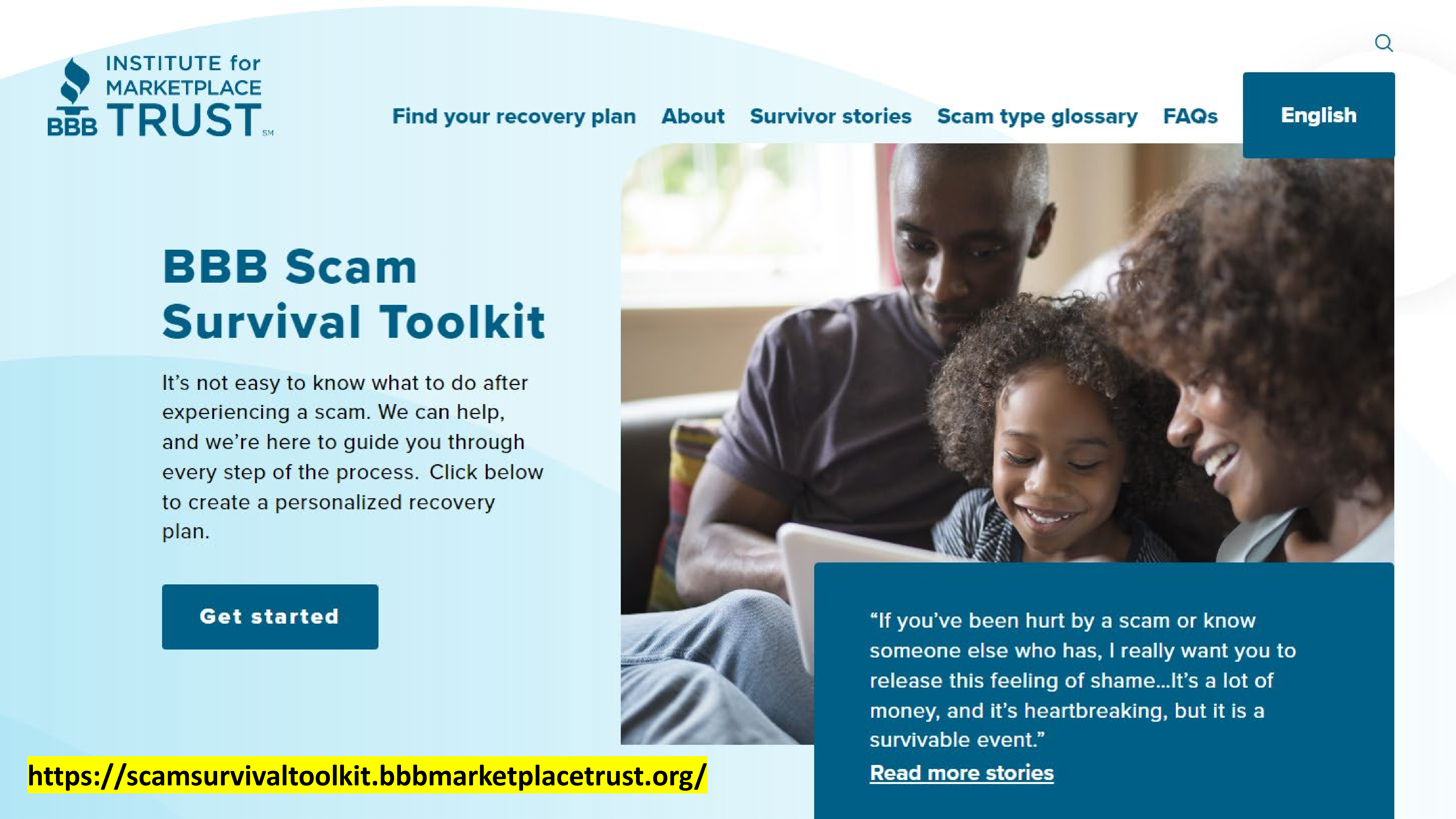
First, if you believe you have fallen victim to cyber crime, file a complaint or report. Your information is invaluable to helping the FBI and its partners bring cybercriminals to justice.

Second, get educated about the latest and most harmful cyber threats and scams. By doing so, you will be better able to protect yourself, your family, and your place of work.

Anyone can become a victim of internet crime. Take action for yourself and others by reporting it. Reporting internet crimes can help bring criminals to justice and make the internet a safer place for us all.

Join the fight against internet crime!

https://www.ic3.gov/



BBB Scam Survival Toolkit

It's not easy to know what to do after experiencing a scam. We can help, and we're here to guide you through every step of the process. Click below to create a personalized recovery plan.

"If you've been hurt by a scam or know someone else who has, I really want you to release this feeling of shame...It's a lot of money, and it's heartbreaking, but it is a survivable event."

Read more stories

https://scamsurvivaltoolkit.bbbmarketplacetrust.org/

Thank You!

Questions?

Visit: www.mdcashacademy.org/

Reach out:
Christina Figueroa,
christina@cashmd.org

https://www.surveymonkey.com/r/VirtualFinEd24Q1

Creating Assets, Savings and Hope

CASH CAMPAIGN OF MARYLAND