



Privacy and Security in the Age of AI

Presentation 101

Lakeland Cybersafe

A Community Project

Presentations – Focus Areas

- **Total 4 presentations (101 and 102 are basic, for everyone)**
 - **Presentation 101 – Easy steps for the most protection**
 - **Presentation 102 – Various kinds of scams, malware**
 - **Presentation 201 – A little technical (VPNs, privacy)**
 - **Presentation 301 – A little more technical (Routers, IoT)**
- **All presentations are online at LakelandCybersafe.org**
- **Links to articles and more resources on the website**

Presentation 101 – Outline

- **Overview of the current situation – facts and trends**
- **What we can do as individuals to protect ourselves**
- **The big picture – a typical home setup (devices, router)**
- **The Wild Wild World Wide Web – the Dark Web**
- **Concrete steps you can take today after this presentation**
 - Maintain password hygiene, Set up 2-Factor Authentication (2-FA)
 - Watch out for identity theft
 - Prevent SIM swapping scams

Questions?

- Please feel free to interrupt at any time to ask questions!
- It's not a lecture. Let's make it lively and interactive!
- I'll be around after the presentation for more questions



Cybercrime Data and Reports

 BD Emerson

Services ▾ Industries ▾ Cases About Blog

  Book a Call

In this article:

- Cyber Crime Statistics Overview: Key Figures for 2026
- Cybercrime Cost Statistics
- The Most Common Cybercrimes
- Top 10 U.S. States by Victims of Cybercrime and Financial Losses (2023)
- Cybercrime Preparedness: Key Statistics and Predictions
- Cyber Crime Trends
- Conclusion
- Take the next step toward protecting your business
- Resources

Home / Blog / Cybercrime Statistics 2026: Cost, Threats & Trends

Cybercrime Statistics 2026: Cost, Threats & Trends

Cybersecurity / April 23, 2026



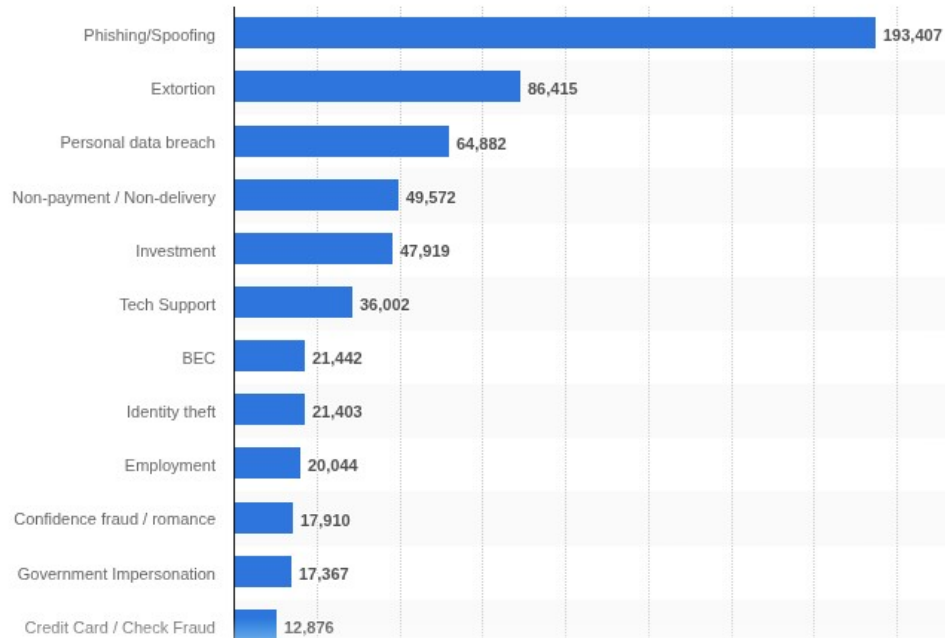
Key Trends

- At \$10 Trillion in damages, third largest economy in the world
- The FTC received 6.47 million cybercrime reports in 2024, with: 40% related to fraud and 18% involving identity theft
- Americans ages 60+ filed 201,266 cybercrime complaints in 2025 and lost \$7.75 billion — a 59% annual increase. The average loss per senior was \$38,500, with 12,400 losing more than \$100,000 each.
- Cybercrime is a relentless threat, with over 2,348 attacks occurring every single day - amounting to nearly 850,000 cyber attacks annually

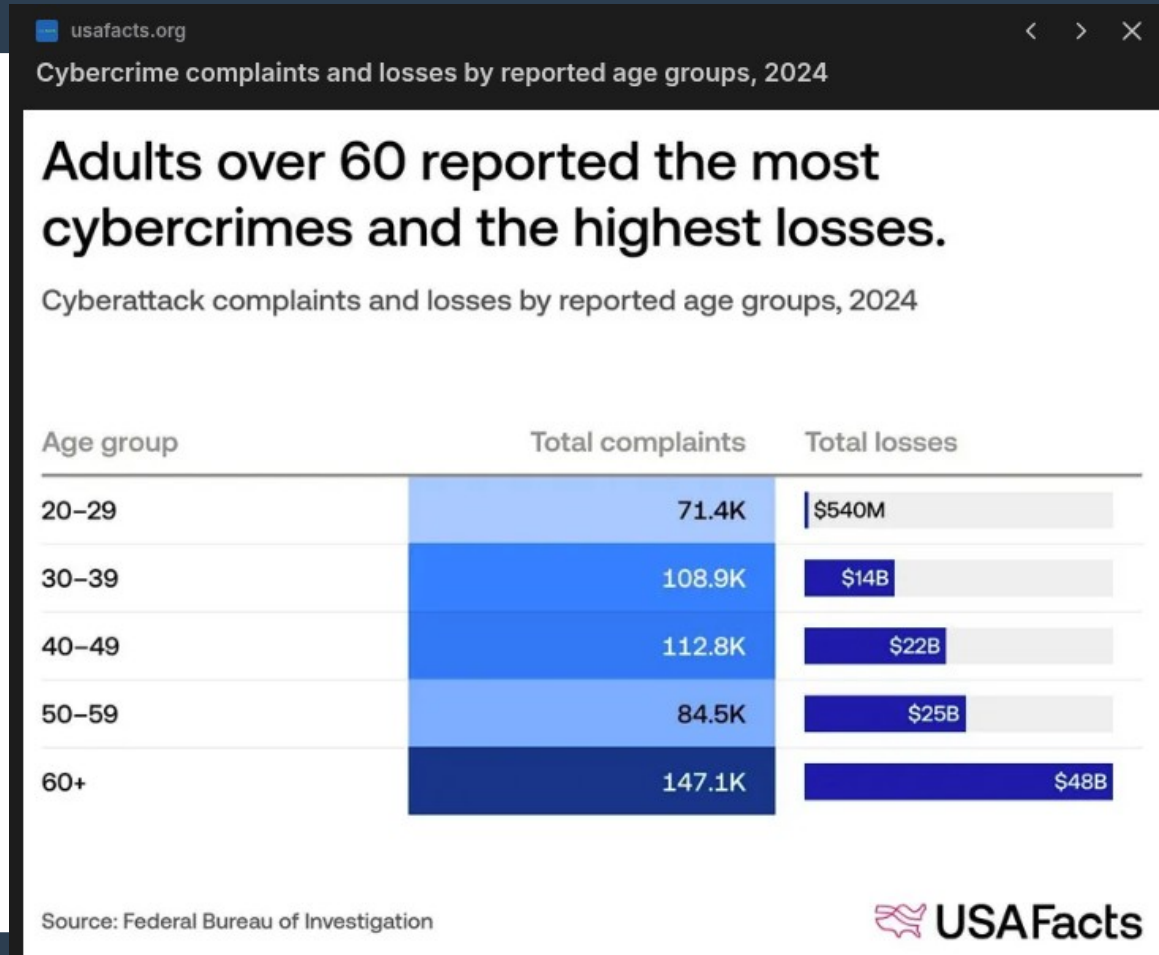
Most Common Cybercrimes

Internet › Cyber Crime & Security

Most commonly reported cybercrime categories in the United States in 2024, by number of individuals affected



Cybercrime Victims by Age Group



Fraud Reports by Contact Method

FTC fraud reports by contact method, number, and median loss*

Method	Number	Median loss
Email	186,621	\$400
Mail	35,878	\$799
Online ad/pop-up	6,884	\$172
Other	100,926	\$234
Phone call	383,598	\$1,170
Social media	70,365	\$200
Text	334,524	\$800
Website/App	134,416	\$150

Cybercrime Victims by State

Cybercrime victims per 100,000 population

Highest		Lowest	
Nevada	523	Mississippi	83
District of Columbia	302	South Dakota	88
Iowa	297	North Dakota	100
Alaska	283	West Virginia	106
Florida	250	Louisiana	109

Cybercrime Activity on the Rise

- **AI is enabling fraud at scale. Hacker collectives run like businesses with their own HR departments and recruiting**
- **3.4 billion phishing emails sent daily, 82.6% are AI-generated**
- **AI being used to clone voices, images and text**
- **Attackers increasingly motivated as much by peer prestige as by money. Bragging rights on social networks**
- **Law Enforcement and corporate information security departments are doing everything they can to mitigate the threat but individual responsibility is paramount**

Government and Law Enforcement Efforts

- **Federal**
 - **FBI's Internet Crime Complaint Center (IC3)**
- **Florida State**
 - **Florida Department of Law Enforcement's Computer Crime Center**
- **Polk County**
 - **AI Investigative Unit launched in June 2024 by the Polk County Sheriff's Office (PCSO) in partnership with Florida Polytechnic University. AI-related crimes, including cyber harassment, identity theft, extortion, hate crimes, and deepfake misuse**
- **Lakeland**
 - **The Lakeland Police Department's General Crimes Unit investigates local computer and internet-related theft and fraud**

What can we do as Individuals?

Awareness

-

Assistance

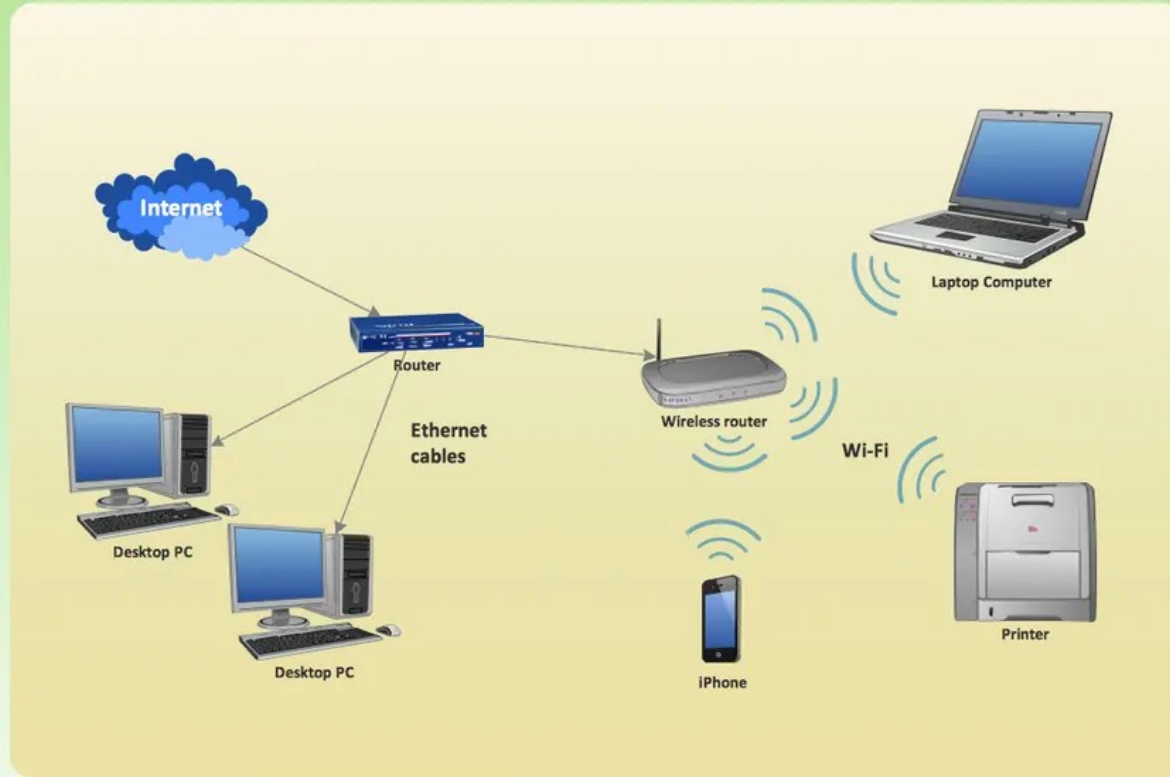
-

Advocacy

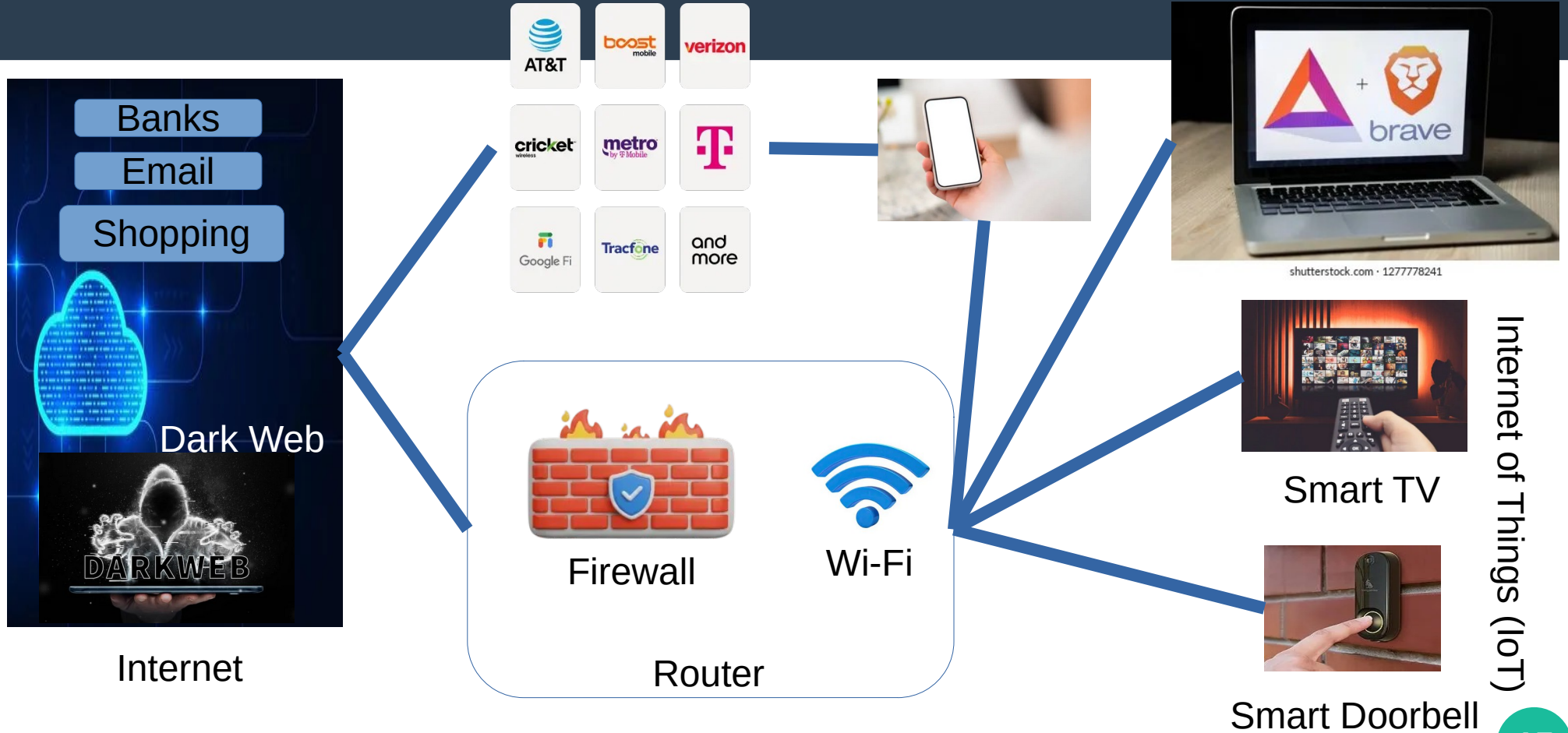
- Educate ourselves on the fast-evolving threat landscape
- Subscribe to cybersafety newsletters, discuss with others
- Take steps to secure your accounts and devices
- Help each other get secure to make the community safer
- Reach out to family and friends to impress upon them the importance of entering a “cybersafe mindset”!

Typical Home Set-up

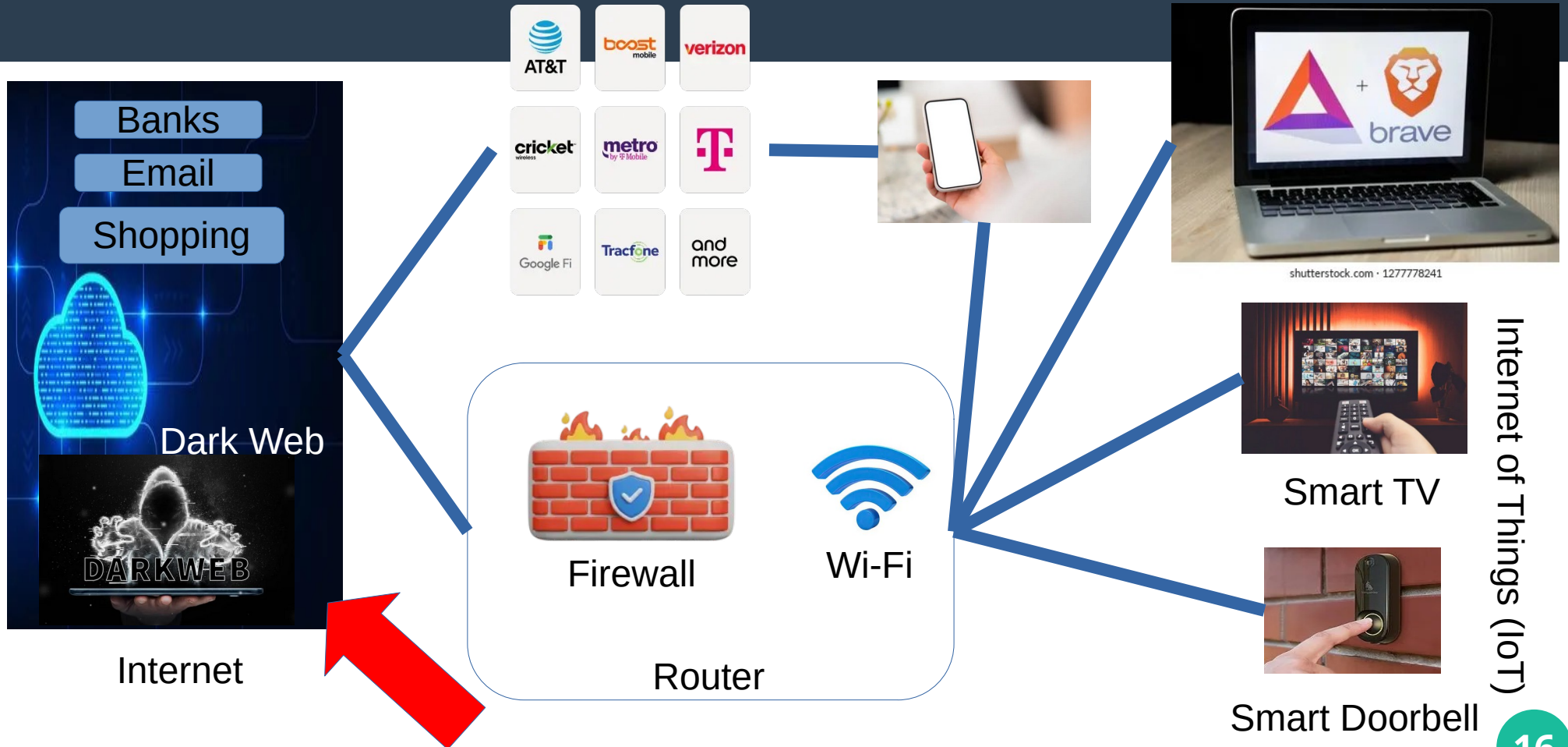
Two Router Home Network Diagram



The Big Picture



The Big Picture



The World Wide Web

- **Dark Web – where hackers sell stolen passwords, account information, personal data like Social Security Numbers**
 - A number of secret marketplaces where illegal activity happens
- **Passwords**
- **2-FA (2-Factor Authentication)**
 - 2-FA - Most important for email accounts and online banking
- **Data removal services (Incogni, Optery, DeleteMe)**
- **Identity Theft**

The World Wide Web

- **Dark Web – where hackers sell stolen passwords, account information, personal data like Social Security Numbers**
 - A number of secret marketplaces where illegal activity happens
- **Passwords**
- **2-FA (2-Factor Authentication)**
 - 2-FA - Most important for email accounts and online banking
- **Data removal services (Incogni, Optery, DeleteMe)**
- **Identity Theft**



by **Darren Guccione**
Contributor

What is the dark web? How to access it and what you'll find

Opinion

Apr 2, 2024 • 14 mins

The dark web is part of the internet that isn't visible to search engines and requires the use of an anonymizing browser called Tor to be accessed.

[Related content](#)

What can you buy on the dark web?

You can buy credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts and software that helps you break into other people's computers. Buy login credentials to a \$50,000 Bank of America account, counterfeit \$20 bills, prepaid debit cards, or a "lifetime" Netflix premium account. You can hire hackers to attack computers for you. You can buy usernames and passwords.

Not everything is illegal, the dark web also has a legitimate side. For example, you can join a chess club or BlackBook, a social network described as the "the Facebook of Tor."

Note: This post contains links to dark web sites that can only be accessed with the Tor browser, which can be downloaded for free at <https://www.torproject.org>.

Private Data for Sale

As in the real world, the price you pay for stolen data fluctuates as the market changes. According to Privacy Affair's Dark Web Price Index 2021, these are the most current prices for some of the data and services commonly traded over the dark web:

- Cloned credit card with PIN: \$25 to \$35
- Credit card details with account balance up to \$5,000: \$240
- Stolen online banking logins with at least \$2,000 in the account: \$120
- PayPal transfers from stolen accounts: \$50 to \$340
- Hacked Coinbase verified account: \$610
- Hacked social media account: \$1 to \$60
- Hacked Gmail account: \$80
- Hacked eBay account with good reputation: \$1,000

The World Wide Web

- **Dark Web – where hackers sell stolen passwords, account information, personal data like Social Security Numbers**
 - A number of secret marketplaces where illegal activity happens
- **Passwords**
- **2-FA (2-Factor Authentication)**
 - 2-FA - Most important for email accounts and online banking
- **Data removal services (Incogni, Optery, DeleteMe)**
- **Identity Theft**

Password Attacks

- **Microsoft blocking over 600 million password attacks daily**
 - 7,000 password attacks per second
- **Attack Methods: The majority of these attacks utilize password spraying, phishing, and brute force techniques, often exploiting reused or weak credentials**
- **88% of Basic Web Application attacks involved stolen credentials. Specops's 2026 Breached Password Report analyzed more than 6 billion passwords stolen by malware in 2025 alone**
- **Microsoft's Digital Defense Report 2025 confirmed that more than 97% of identity attacks are password attacks and that identity-based attacks surged 32% in H1 2025**

Password Hygiene

- **Password strength – min 8 characters (hard to guess)**
- **Password reuse – highly discouraged**
 - Stolen passwords are all over the dark web
- **Saving passwords in the browser – not recommended**
- **Password Managers - depends**
- **Most important password is the one for the email account**
- **Remember: passwords can be guessed/cracked by bots**

Password Manager LastPass Hacked

Forbes

INNOVATION > CYBERSECURITY

LastPass Data Breach — 1.6 Million Users Exposed By Security Failure

By [Davey Winder](#), Senior Contributor. © Davey Winder is a veteran cybersecur... [▼](#)

[Follow Author](#)

Published Dec 14, 2025, 07:36am EST, Updated Dec 14, 2025, 07:52am EST



FORBES' FEATURED VIDEO

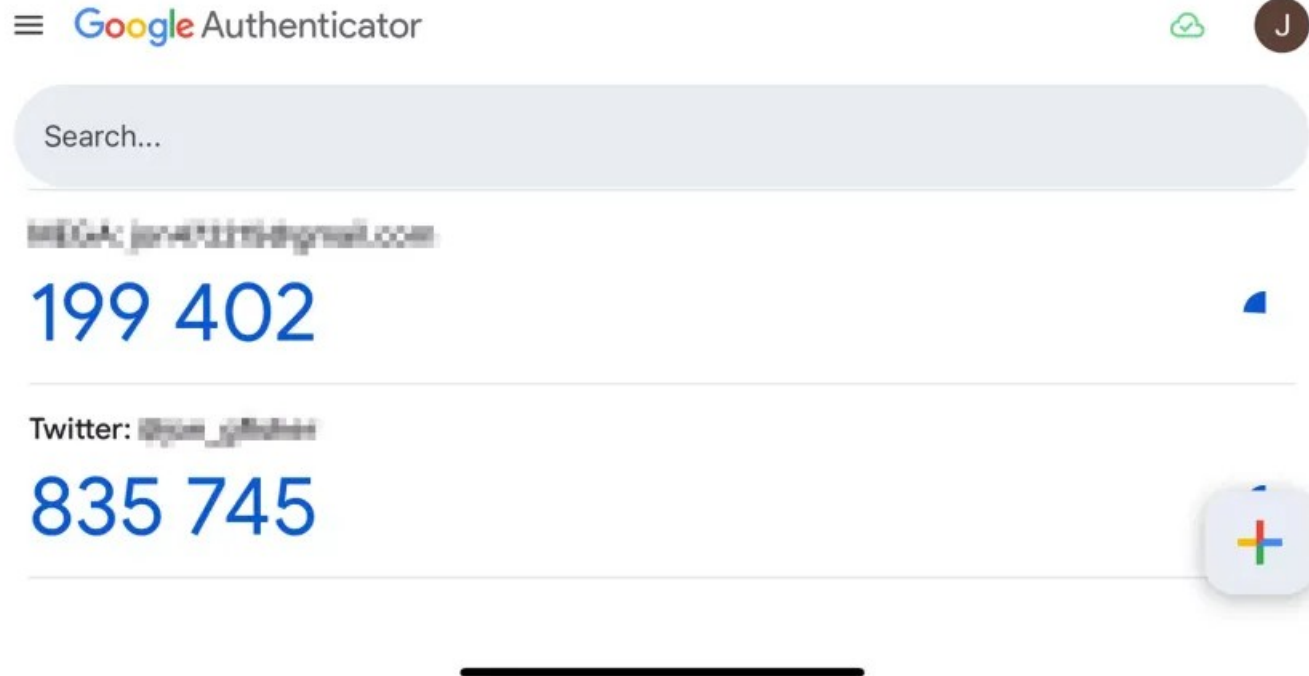
The World Wide Web

- **Dark Web – where hackers sell stolen passwords, account information, personal data like Social Security Numbers**
 - A number of secret marketplaces where illegal activity happens
- **Passwords**
- **2-FA (2-Factor Authentication)**
 - 2-FA - Most important for email accounts and online banking
- **Data removal services (Incogni, Optery, DeleteMe)**
- **Identity Theft**

2-Factor Authentication

- **Password = Something you know (1st factor)**
- **2nd factor = Something you have (a phone, bio-metrics, UbiKey)**
 - Stronger security when both password and 2nd factor are used
- **Most common 2nd factor = OTP via text message to your phone**
- **Next most common = Authenticator Apps (Example: Google Authenticator)**
- **Passkey (bio-metrics built into the phone)**
- **Physical key (UbiKey)**

Google Authenticator



UbiKey

yubico
YubiKey 5 Series



Multi-protocol lineup that is the #1 choice for businesses and supports passwordless



The World Wide Web

- **Dark Web – where hackers sell stolen passwords, account information, personal data like Social Security Numbers**
 - A number of secret marketplaces where illegal activity happens
- **Passwords**
- **2-FA (2-Factor Authentication)**
 - 2-FA - Most important for email accounts and online banking
- **Data removal services (Incogni, Optery, DeleteMe)**
- **Identity Theft**

Data Removal Services



Privacy Settings – Say “No No No”

[View the HP Privacy Statement to learn more about HP's privacy practices and your data rights.](#)

HP collects and processes data to deliver functionality. All personal data will be processed in accordance with the HP Privacy Statement.

Choose your HP privacy settings below.

Yes to All

No to All

I consent to HP using information about my system to provide me with customer support and to enable my PC to show HP contact options, warranty information, and important support messages.

☐

Yes

☒

No

I consent to HP using information about my system to improve HP products and services.

[What System Information Does HP Collect?](#)

☐

Yes

☒

No

I consent to HP using my data to provide tailored HP and third-party offers and ads. This includes sharing data with partners, service providers and marketing networks to present HP and third-party ads on HP and third-party platforms.

☐

Yes

☒

No

The World Wide Web

- **Dark Web – where hackers sell stolen passwords, account information, personal data like Social Security Numbers**
 - A number of secret marketplaces where illegal activity happens
- **Passwords**
- **2-FA (2-Factor Authentication)**
 - 2-FA - Most important for email accounts and online banking
- **Data removal services (Incogni, Optery, DeleteMe)**
- **Identity Theft**

Identity Thieves can...



Steal money from your
bank and investment
accounts



Cause you to potentially
spend hundreds of hours
to restore your identity



Obtain tax refunds using
your identity



Take out loans in your
name



Ruin your good credit



Commit criminal acts
using your identity

Identity Theft

Every two seconds, someone in the U.S. becomes a victim of identity theft.

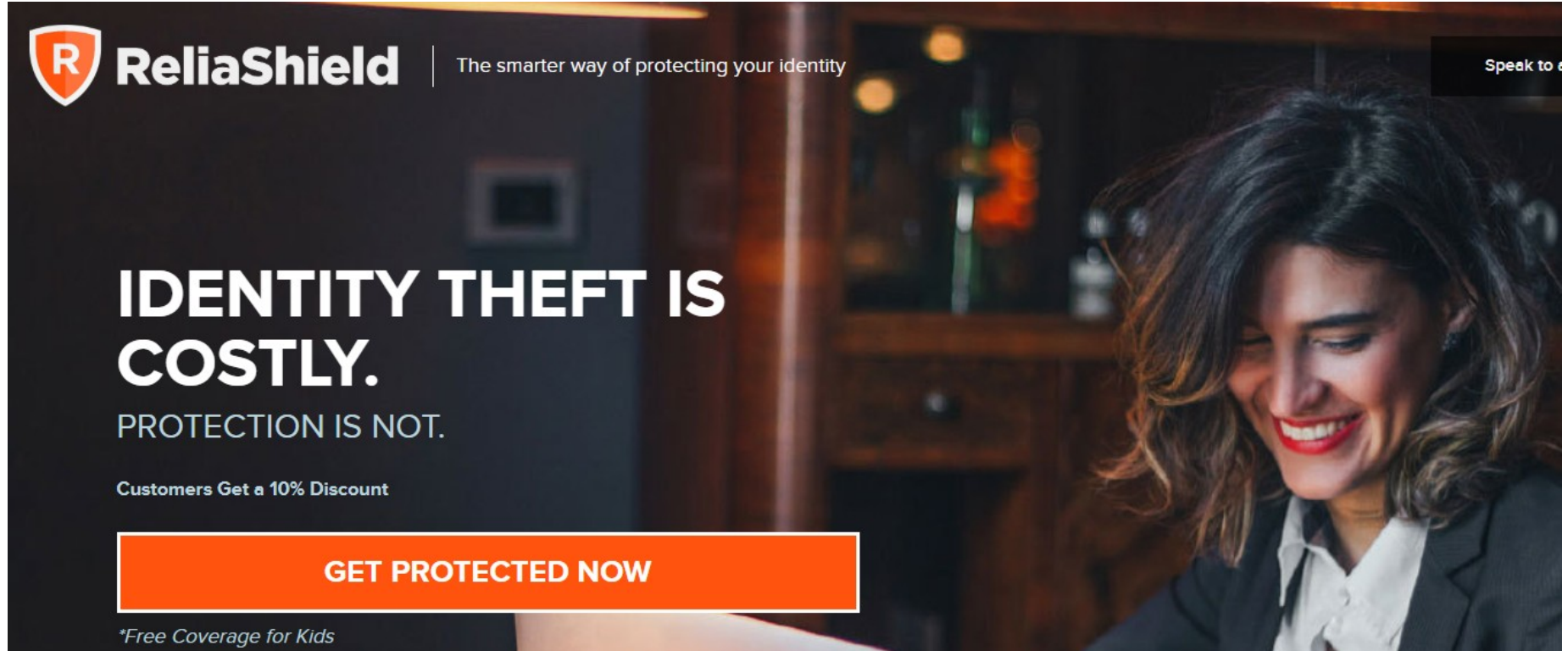
THERE WERE
**18
MILLION**
ID THEFT VICTIMS
IN THE US IN 2024

**\$27
BILLION**
WAS STOLEN BY
IDENTITY THIEVES
IN 2024

CONSUMERS USING
SOCIAL MEDIA
HAVE A
46%
HIGHER RISK OF
ACCOUNT TAKEOVER

THERE WERE
**1.3
BILLION**
INDIVIDUAL RECORDS
EXPOSED IN DATA BREACHES
-JUST IN THE US

Identity Theft



ReliaShield | The smarter way of protecting your identity

IDENTITY THEFT IS COSTLY.
PROTECTION IS NOT.

Customers Get a 10% Discount

GET PROTECTED NOW

**Free Coverage for Kids*

Speak to a

Credit Reports - Easiest Way to Detect Identity Theft



FREE Credit Reports. Federal law allows you to:



- Get a free copy of your credit report every 12 months from each credit reporting company.



- Ensure that the information on all of your credit reports is correct and up to date.

AnnualCreditReport.com

AnnualCreditReport.com

The only source for your free credit reports. Authorized by Federal law.

Home

All about credit reports

Request yours now!

What to look for

Protect your identity

Frequently asked questions

Contact us



Free weekly online credit reports are available from Equifax, Experian and TransUnion. Credit reports play an important role in your financial life and we encourage you to regularly check your credit history.

[Request your free credit reports](#)

Don't be fooled by look-alikes.

Lots of sites promise credit reports for free.
AnnualCreditReport.com is the only official site explicitly directed by Federal law to provide them.

[About AnnualCreditReport.com](#)



Legal Experts' Recommendation

The screenshot shows the top of a website for Raburn Kaufman. The header includes the firm's logo on the left, a navigation menu with links for Services, About, Results, Resources, and Contact in the center, and a tagline 'If We Don't Win, You Don't Pay!' with the phone number 877-662-2455 on the right. Below the header, a date line indicates '03/19/2026'. The main headline reads 'Why Checking AnnualCreditReport.com Should Be Part of Your Financial Routine'. At the bottom, there is a photo of a man looking at a credit report and a call-to-action button that says 'Get a Free Consultation' with a phone icon and a right-pointing arrow.

RABURN KAUFMAN

Services ▾ About ▾ Results ▾ Resources ▾ Contact

If We Don't Win, You Don't Pay!
[877-662-2455](tel:877-662-2455)

03/19/2026

Why Checking AnnualCreditReport.com Should Be Part of Your Financial Routine

Get a Free Consultation >

Credit Reports - Best Practices

- **Create an account with each of the three agencies (claim your profile)**
 - No need to upgrade to paid/subscription accounts
 - Free credit reports available once per week
- **Best to pull one report every 4 months, rotating between the three agencies**
 - Check all details including addresses and phone numbers
 - Most importantly, check if there are any loans/mortgages that aren't yours
- **Credit monitoring services available for a fee from third parties**

Credit Freeze

[Your Credit](#)[Education](#)[About](#)[Credit Support](#)

Credit Freeze

A credit freeze, also known as a security freeze, helps prevent new accounts from being opened. You're absolutely free to freeze, unfreeze and temporarily thaw your credit, and it won't affect your credit score.

[Add Freeze](#)[Unfreeze](#)

Credit Freeze

 [Personal](#) [Business](#)

[Products & Services](#) [Learn](#) [Credit Offers & More](#)

[Home](#) > [My Personal Credit](#) > [Equifax Consumer Services Center](#) > [Security Freeze](#)

Security Freeze

Placing, temporarily lifting, or removing a security freeze is free.

[PLACE A SECURITY FREEZE](#)[MANAGE A FREEZE](#)

Fraud Alert



Credit ▾

Protection ▾

Money ▾

Credit Cards ▾

Loans ▾

Insurance ▾

Sign in

Fraud Alert

Fraud alerts notify creditors to verify your identity before extending credit in case someone is using your information without your consent.

Manage your fraud alert for free

New to Experian? Sign up.

Create a free account

Federal Trade Commission Advisory



FEDERAL TRADE COMMISSION
CONSUMER ADVICE

Shopping and
Donating ▾

Credit, Loans,
and Debt ▾

Jobs and
Making Money ▾

Unwanted Calls,
Emails, and Texts ▾

Identity Theft and
Online Security ▾

[Home](#) / [Articles](#)

[Vea esta página en español](#)

Article

Credit Freezes and Fraud Alerts

Credit freezes and fraud alerts can help protect you from identity theft by making it harder for scammers to open new credit accounts in your name. They can also help stop someone who already stole your identity from misusing it again. Here's what to know about what credit freezes and fraud alerts do and how to use them.

FTC Resources



FEDERAL TRADE COMMISSION
CONSUMER ADVICE

Shopping and
Donating ▾

Credit, Loans,
and Debt ▾

Jobs and
Making Money ▾

Unwanted Calls,
Emails, and Texts ▾

Identity Theft and
Online Security ▾

Scams

Identity Theft and Online Security

How to protect your personal information and privacy, stay safe online, and help your kids do the same.

[Vea esta página en español](#)

Identity Theft

How to protect your personal information from identity theft.

Online Privacy and Security

Understanding online privacy, how to protect your devices from hackers and

Protecting Kids Online

How to talk to your kids about being online, and how to help them make good

Florida Government Advisory



**Florida Department of
Agriculture and Consumer Services**
Commissioner Wilton Simpson

[My Settings/Profile](#)

[File a Complaint](#) [Pay/Register Online](#) [Forms](#) [By Topic ▼](#) [Our Department ▼](#) [Search](#)

[Home](#) / [Consumer Resources](#) / [Identity Theft](#) / Identity Theft

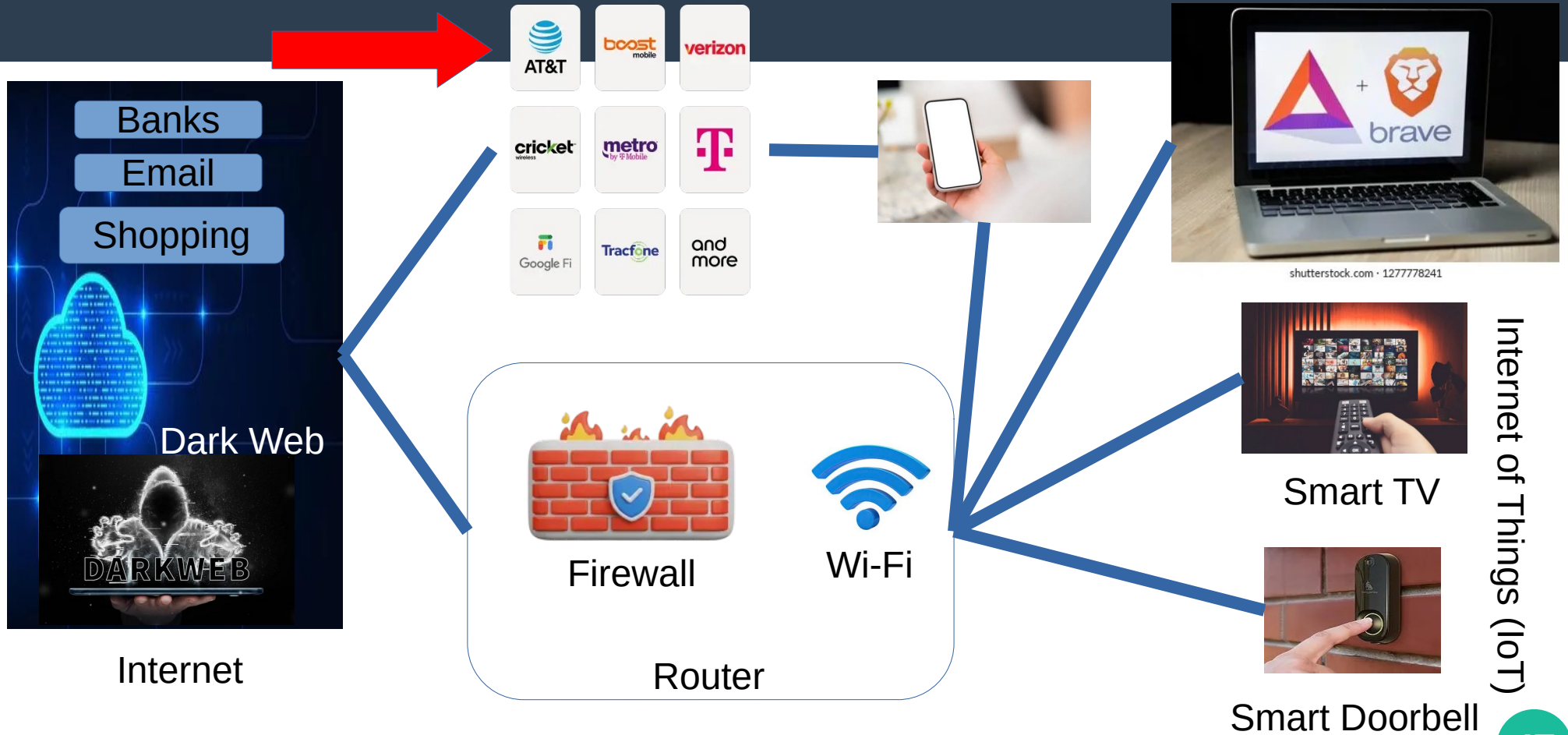
Identity Theft

Identity theft occurs when an individual's personal information (such as their name, Social Security number or credit card number) is used without their consent to commit fraud and other crimes. The Federal Trade Commission (FTC) estimates that as many as 10 million Americans have their identities stolen each year.

Identity Theft

[Security Freeze](#) — [Credit Report FAQ](#)

The Big Picture



SIM Swapping



What is a SIM Card?



SIM Swapping Fraud



©2025 Trend Micro

SIM Swapping Fraud – Tell-tale Sign

Your phone



Attacker's phone



A SIM swap will deactivate your phone, and if done by an attacker, the attacker will receive your calls and texts on thier device.

SIM Swapping Fraud on the Rise



[The Wireless Industry](#)

[Positions](#)

[Consumer Resources](#)

[News](#)

[About CTIA](#)

 [Search](#)

Consumer Resources

Protecting Your Wireless Account Against SIM Swap Fraud.



FEDERAL TRADE COMMISSION
CONSUMER ADVICE

Shopping and
Donating ▾

Credit, Loans,
and Debt ▾

Jobs and
Making Money ▾

Unwanted Calls,
Emails, and Texts ▾

Identity Theft and
Online Security ▾

Scams



[Home](#) / [Consumer Alerts](#)

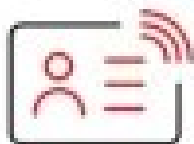
[Vea esta página en español](#)

Consumer Alert

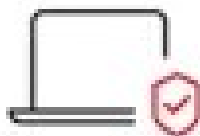
SIM Swap Scams: How to Protect Yourself

Protect Yourself from SIM-swapping Attempts

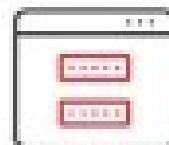
How to Protect Yourself from SIM Swapping Attacks



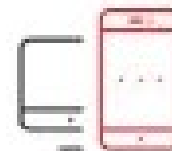
Limit Personal
Information Shared
Online



Monitor Your
Accounts Proactively



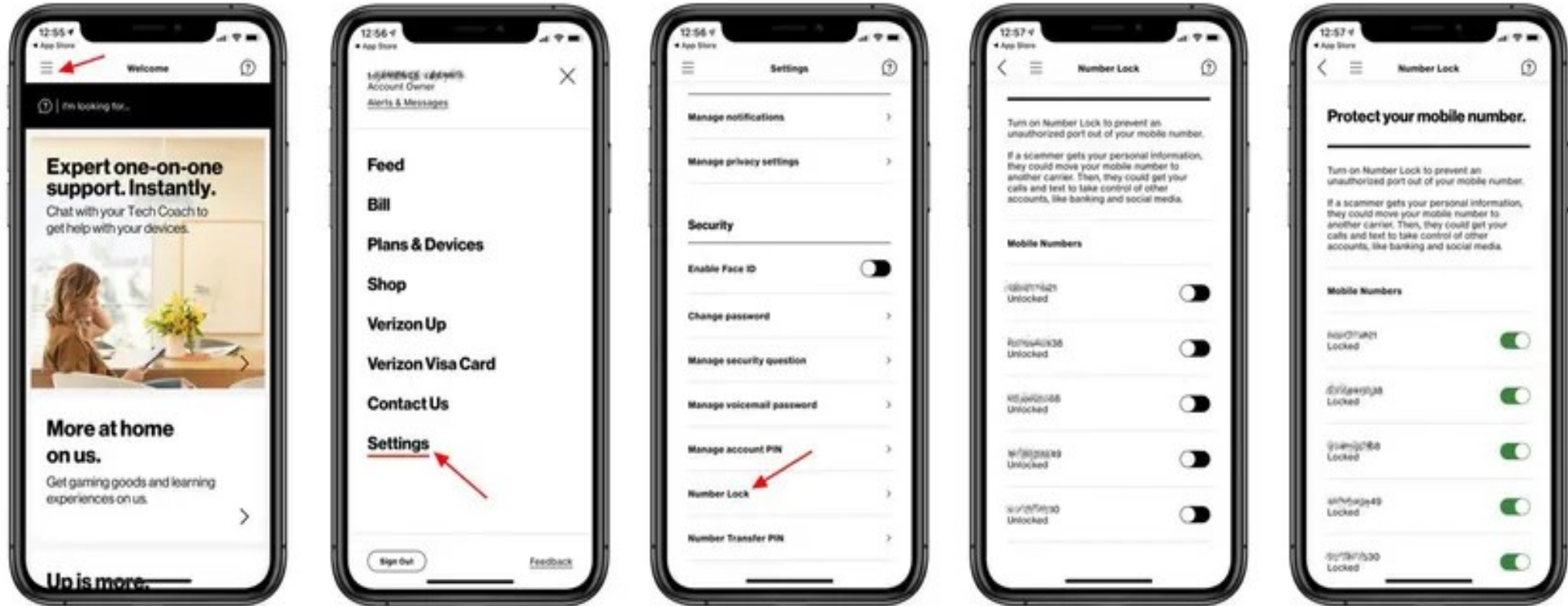
Set Up a Carrier-Level
PIN or Port Lock



Use App-Based
or Hardware
2FA Instead of SMS

©2025 Trend Micro

Verizon Carrier Settings – Number Lock



Spectrum Carrier Settings – Number Lock

Home

Billing

Services

Upgrade

Support

More

Chat With Us

Settings

Your Info

Sign In & Security

People

Notifications

Username

Password

>

Security Question

>

Security Code

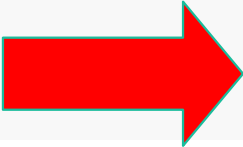
>

Account Fraud Protection

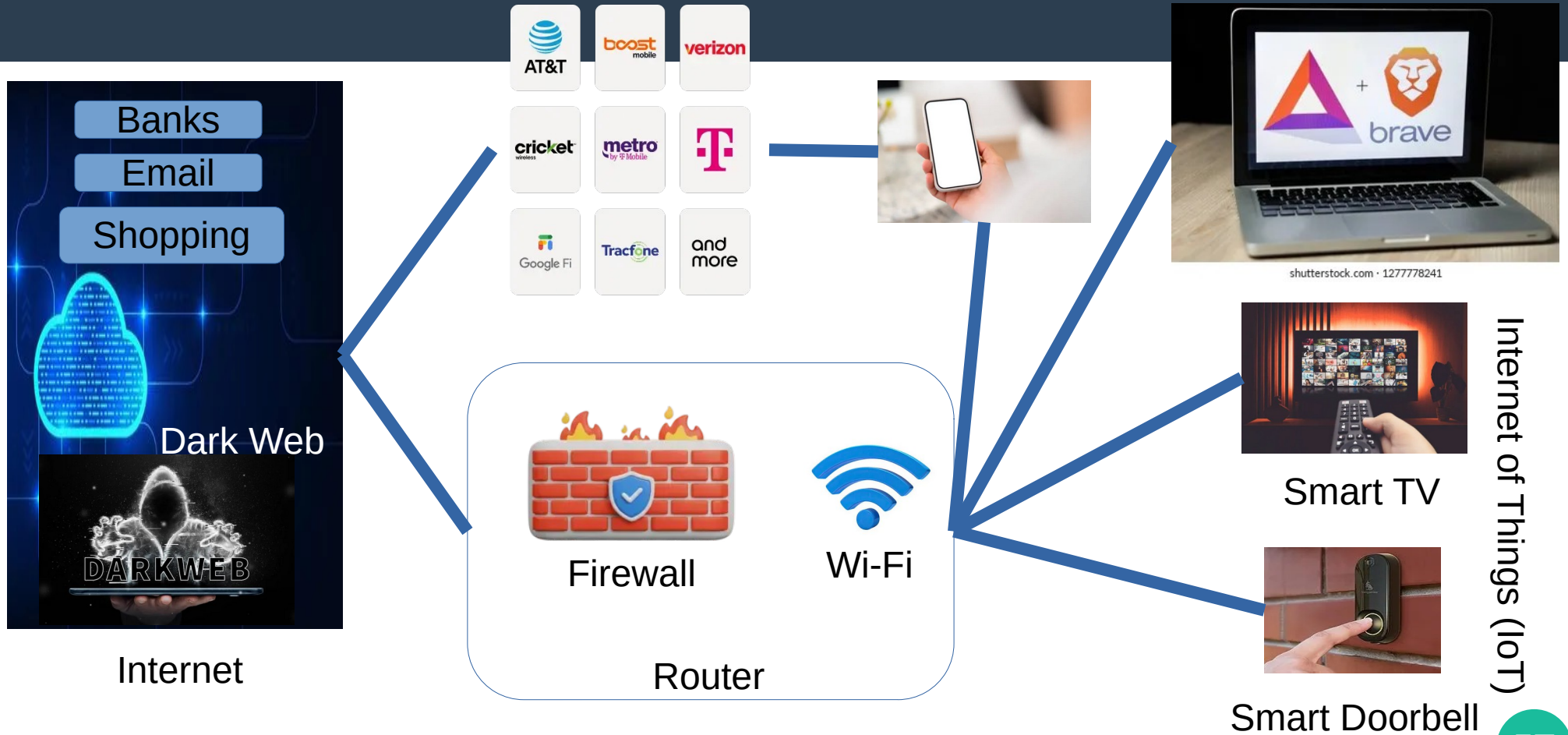
>

Safeguard against fraud by locking device switching and transfer PINs.

On



The Big Picture



Preview of Presentation 102

- Understanding various forms of scams and attacks – phishing, impersonation, malware, hacking
- Privacy and security settings on your devices
- Introduction to Virtual Private Networks (VPNs)
- Entering and staying in the “cybersafe mindset”
- Online tools and resources

Thank you!

