



Privacy and Security in the Age of AI

Presentation 102

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 102 – Outline

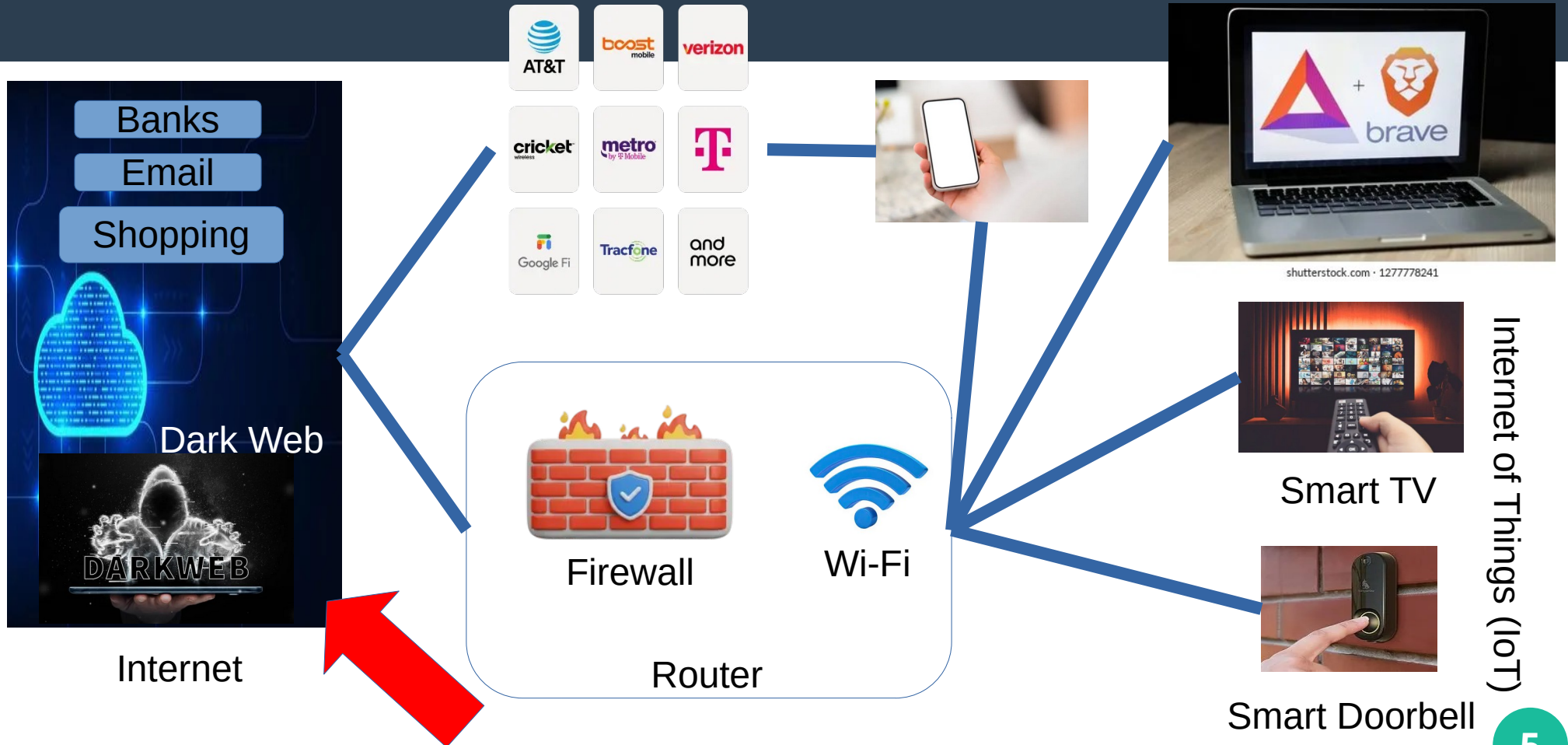
- Understanding various forms of scams and attacks – phishing, impersonation, malware, hacking
- Privacy and security settings on your devices
- Introduction to Virtual Private Networks (VPNs)
- Entering and staying in the “cybersafe mindset”
- Online tools and resources

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



The Big Picture



A Typical Call Center(?)



Cyber Scams

- **Cyber scams are deceptive schemes that use one or more of these communication channels**
 - Phone/Voice, Email/Text, Social Media, or Websites and other electronic means
- **to steal one or more of**
 - Private information, Account access, or Money
- **They generally exploit human psychology (social engineering) or technical vulnerabilities**
 - They come in many shapes and varieties
 - Some are easier to spot than others
 - Don't include other cyber menaces like cyber-bullying or relationships with AI models

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

Some Common Types of Scams

- **Tech Support Scam:** Scammers pose as customer service or IT experts, claiming they can help you with account issues or malware removal
- **Phishing and Identity Theft:** Unsolicited messages trick victims into revealing Social Security numbers, bank details, or login credentials
- **Distress Scams:** High-pressure hurried situations where a loved one is in distress (accident, arrest etc.) and needs money immediately
- **Romance/Confidence Scams:** Exploiting loneliness to build trust before extracting money or personal data
- **Investment and Crypto Scams:** High-pressure schemes promising guaranteed returns or exploiting lack of technical oversight

Windows Defender Alert : Zeus Virus Detected In Your Computer !!

Please Do Not Shut Down or Reset Your Computer.

The following data will be compromised if you continue:

1. Passwords
2. Browser History
3. Credit Card Information
4. Local Hard Disk Files.

This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks.

Call Technical Support Immediately at +1-877-219-6702



Call Microsoft Technical Department: +1-877-219-6702 (Toll Free)

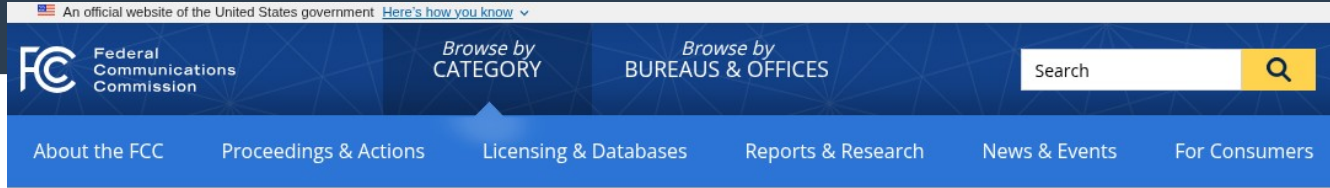




Tech Support Scams

- **Scammers pose as customer service or tech support personnel and trick the victim into revealing their login credentials or install remote-access software**
 - May use “spoofing” to appear legitimate (caller ID, sender email address)
 - Commonly target seniors and others who are not computer savvy
 - Sometimes impersonate large technology companies or even federal authorities like the FBI and the IRS
 - Attempt to gain access to our computer by having us install remote-access software like RustDesk, AnyDesk and TeamViewer

Caller ID Spoofing



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

Caller ID Spoofing

[Español](#) | [한국어](#) | [繁體中文](#) | [Tagalog](#) | [Tiếng Việt](#)



FCC Consumer Video: Don't Hang On, Hang Up! To [watch this video with captions](#), hit play, click on the settings icon, then click "Subtitles/CC" and select from available languages.

What Is Spoofing?

Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often use neighbor spoofing so it appears that an incoming call is coming from a local number, or spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity.

Watch the video and click through the tabs to learn more about spoofing and how to avoid being scammed.

If you think you've been the victim of a spoofing scam, you can [file a complaint with the FCC](#).

Remote-Access Software

- **Legitimate software programs used by individuals and companies that allow...**
 - Employees to login into their work computers from home or a remote location
 - Legitimate tech support personnel (or a trusted friend) to access our computer to help us troubleshoot problems
 - Full access to our computer or phone (what they see is what we see) including control of mouse and keyboard

Remote-Access Software Warning

WARNING: YOU MAY BE BEING SCAMMED!

If you are on the phone with someone you DON'T know AND TRUST who has asked you to install RustDesk, do not install and hang up immediately.

They are likely a scammer trying to steal your money or other private information.

NEW Enhanced ACL in RustDesk Server Pro 1.5.0! »



Resources ▾

Pricing

Docs

Blog



Note: rustdesk.com is our only official domain. Please do not download RustDesk from the other domains.

The Fast Open-Source Remote Access and Support Software

Switch from TeamViewer, AnyDesk, and Splashtop to RustDesk for a secure and reliable remote desktop experience with your own self-hosted servers.

Download ↓

Self-Hosting ☰

Remote-Access Software Warning

From Wikipedia, the free encyclopedia

AnyDesk is a [remote desktop application](#) distributed by AnyDesk Software GmbH. The [proprietary](#) software program provides platform-independent remote access to [personal computers](#) and other devices running the host application.^[10] It offers remote control, [file transfer](#), and [VPN](#) functionality. AnyDesk is often used in [technical support scams](#) and other remote access scams.^{[11][12][13]}

**AnyDesk**

[Developer](#) AnyDesk Software [GmbH](#)

[Stable release\(s\)](#) ^[±]

Windows 9.7.8 / June 25, 2026; 2 days ago^[1]

How to Avoid Tech Support Scams

- **Never engage with unsolicited contacts**
 - Legitimate tech companies like Microsoft don't make unsolicited calls or send emails claiming your computer has problems
- **If you see a pop-up warning on your computer or phone, do not call any displayed phone number or click any links**
 - Take a picture or screenshot and restart your computer or phone immediately
- **Install anti-virus software and keep it updated**
- **Never install remote-access software nor let anyone control your computer even if they claim your computer is infected**

Phishing and its Siblings

- **Scammers impersonate trusted entities to steal login credentials and private information or install malware**
 - Phishing: Deceptive emails directing victims to fake websites or malicious attachments
 - Smishing: Phishing conducted via text messages (SMS)
 - Vishing: Voice phishing using phone calls or voice messages to extract sensitive personal information
 - Quishing: Scams using QR codes to redirect users to malicious sites or trigger unwanted actions on devices

Phishing – Example 1

^ Important Notice



Fri 6/5/2026 8:37 AM

Important Notice

To

 If there are problems with how this message is displayed, click here to view it in a web browser.

We've noticed that your university Microsoft 365 account is set for deactivation due to a recent change in your status (like graduation, withdrawal, or transfer). However, recent activity suggests you might still be connected to the university. To ensure you don't lose access to your account and services, please confirm your current affiliation.

Your access to the following services is at risk:

- University Email (Outlook)
- Microsoft Teams
- OneDrive (cloud storage)
- Office apps (Word, Excel, PowerPoint, etc.)



[\[Verify My Account Now\]](#)

Please Note : **VOLS** means Type Your PASSWORD

Please Note : **VOLS** means Type Your PASSWORD

Note: When prompted for "Email Keyword", enter the **password you currently use to log into your university email account.** (PROTECTED BY ADMIN)

Action required: Please verify your status within 48 hours to avoid permanent deactivation of your Microsoft 365 account. If you do not respond in time, all associated data will be deleted and cannot be recovered.

Phishing – Example 2



Dear User,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active follow the link Sign in Re-activate your account to Outlook. <https://account.live.com>
www.rnicrosoft.com

Thanks,

The Microsoft account team

Phishing – Lookalike URLs

www.rnicrosoft.com

www.LjnkedIN.com

www.PayPal.com

www.PayPa1.com

www.G00GLE.com

www.gooogle.com

www.google.myscamsite.com

Θ	θ	Theta	"th" as in "thin"
Ι	ι	Iota	"i" as in "bit"
Κ	κ	Kappa	"k" as in "kite"
Λ	λ	Lambda	"l" as in "love"
Μ	μ	Mu	"m" as in "man"
Ν	ν	Nu	"n" as in "no"
Ξ	ξ	Xi	"x" as in "taxi"
Ο	ο	Omicron	"o" as in "not"
Π	π	Pi	"p" as in "pot"
Ρ	ρ	Rho	"r" as in "right"

Phishing – Lookalike URLs – What Looks Suspicious?

①	https://twittter.com
②	https://google.com.sign-in.info
③	https://paypal.com
④	https://fb.com@n593.biz
⑤	https://secure-gmail.com
⑥	https://twitter.com-issues.support
⑦	https://www.facebook.com.js2awp1lf8xe89770by5cyxqbwewp.gvicw9vl45liecsmcmcut7z95qcms.etz5811eiue348wi0li27dh8jtkku.mx
⑧	https://get-help.page?google.com https://192.17.42.13#google.com
⑨	https://connection22.co/facebook.com

Phishing – Lookalike URLs

① Typo-squatting (Attack targeting users' mistyping)	https://twitttter.com
② Subdomain as Domain	https://google.com.sign-in.info
③ IDN Homograph	https://paypal.com
④ HTTP credentials as origin	https://fb.com@n593.biz
⑤ Self-declared secure	https://secure-gmail.com
⑥ Unfamiliar TLC	https://twitter.com-issues.support
⑦ Overrunning Subdomain	https://www.facebook.com.js2awp1lf8xe89770by5cyxqbwewp.gvicw9vl45liecsmcmcut7z95qcms.etz5811eiue348wi0li27dh8jtkku.mx
⑧ Query parameters or Fragment Posing	https://get-help.page?google.com https://192.17.42.13#google.com
⑨ Path Posing	https://connection22.co/facebook.com

How to Recognize a Phishing Email

- **Generic greetings:** Because scammers often target a broad set of victims at one time, they often use generic greetings like "Dear customer," or they may even skip the greeting altogether
- **Grammatical errors:** Phishing emails often contain grammatical errors, misspellings, odd capitalization, and unnatural phrasing. While typos happen, legitimate business emails shouldn't have these mistakes
- **Low-resolution logos or images:** Scammers often use copied logos to appear legitimate, but low-quality, blurry, or improperly sized logos are red flags. Be cautious if a logo looks fuzzy, pixelated, stretched, or requires close inspection to see it clearly
- **Suspicious sender email addresses:** Look closely at the sender's email address. Phishers might create addresses that look similar to a real company, but with a minor typo or extra character. For example, "appel.com" instead of "apple.com."
- **Strange URLs:** Legitimate companies use clear URLs while phishing emails often link to suspicious ones. Hover your mouse over the link to see the URL before you click it
- **Requests for personal information:** Legitimate companies won't ask for sensitive information like passwords or Social Security numbers through email. If an email tells you to verify your account by clicking a link and entering your login details, it's likely a phishing attempt

How to Recognize a Phishing Email - Example

Sent: Monday, May 09, 2016 10:07 AM

To:

Subject: Fwd: [UVa Library - Circulation] VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

Hello User!

We received your instructions to delete your account

1

We will process your request within 24 hours.

All features associated with your account will be lost.

2

To retain your account, kindly Cancel Request to continue using our services

CANCEL REQUEST IMMEDIATELY

3

Thank You,
Account Team

<http://bit.ly/1WTXQzB>

Please do not reply to this message. Mail sent to this address cannot be answered.

4

Phishing Link Checker

[Products ▾](#)[Tools ▾](#)[Pricing](#)[Resources ▾](#)[Industries ▾](#)[MSPs & Resellers ▾](#)[Home](#) / [Tools](#) / [Phishing Link Checker](#)

Phishing Link Checker

[⚙️ Get API key](#)

Enter a full URL or email content with links to check if it's safe before you visit. Our AI-powered, phishing link checker gives real-time results.

Paste URLs or email original content here

[Check](#)

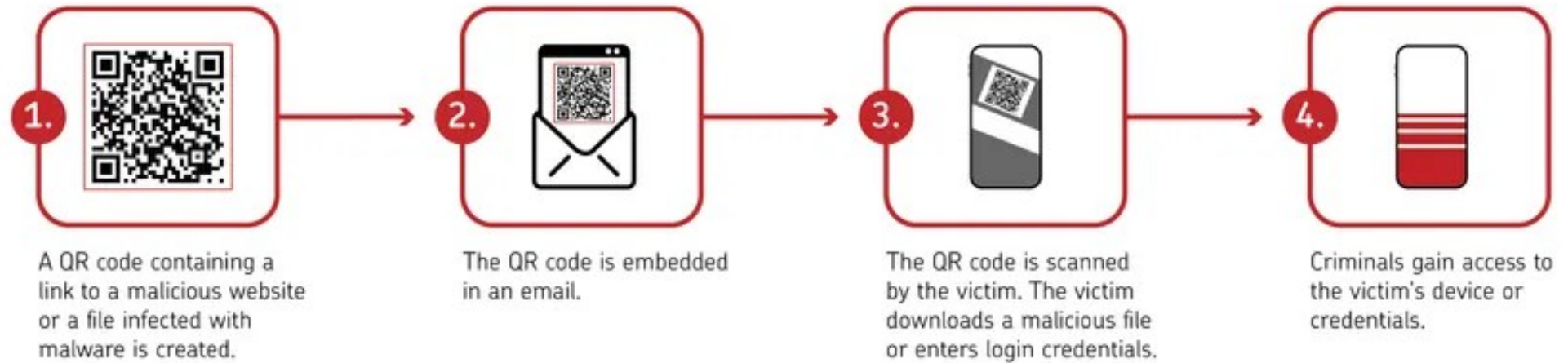
Quishing

- **Quishing (QR code phishing) attacks typically involve social engineering to trick users into scanning a malicious QR code that redirects them to a fraudulent website or triggers a malware download**



Quishing – How it Works

Quishing in a nutshell:



Quishing – Parking Meter Scam



Quishing – Parking Meter Scam



Distress Scams

- **High-pressure hurried situations where a loved one is in distress (accident, arrest etc.) and needs money immediately**
 - While urgency is a factor in most scams, it's central to this type
- **Lately powered by AI voice cloning**
 - A few seconds of a voice sample is enough to create realistic pleas for help which are then played over the phone to create a state of emergency

How to Protect Yourself and Loved Ones

- **Be suspicious of the apparent urgency**
- **Hang up and call the number of the loved one**
- **Agree upon a safe word or phrase which only your family members know**
- **Consult a friend or another family member before acting**
- **Don't engage in dialog – AI can be very convincing**
- **Never send money or crypto**

Romance/Confidence Scams

- **Scammers exploit loneliness to build trust over time before extracting money or personal data**
 - Long-term interaction over months/years before a request for funds
- **Because of the personal bond created, victims lose more than in phishing or ransomware scams**
- **AI being increasingly used to create fake profiles and even hold conversations**
 - Typically begin on social media websites like Facebook or dating apps

Romance/Confidence Scams

- **Tell-tale sign: they always have an excuse for why they can't meet in person or can't even do a video call**
 - Overseas working in the army or a very busy business executive
- **A too-good to believe investment opportunity in cryptocurrency or an emergency eventually shows up**
- **Many of these scams go unreported to friends/authorities because of the shame involved on the part of victims**
 - A trusted friend can help discern if the “relationship” is legitimate

Investment and Crypto Scams

- **High-pressure schemes promising guaranteed returns or exploiting lack of technical oversight**
 - “Special offer valid only until midnight tonight”
- **May initially start with a romance scam**
- **Ponzi schemes that take advantage of the anonymity offered by the Internet and social media websites**
 - Often involves Bitcoin, real estate or startup stocks

Anonymity on the Internet

An
Internet
meme
from
1993



"On the Internet, nobody knows you're a dog."

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

"On the
Internet,
nobody
knows
you're a
dog"

Anonymity on the Internet

Now, the
dog has
learned
to use AI



Bottom-
line:
Careful
who you
trust on the
Internet!

Other Scams

- **Hacking** – when someone breaks into our email, online accounts, computer or phone
- **Ransomware** – when someone breaks in and holds our data hostage and demands payment in return for release
- **Typo-squatting** – reserving lookalike domain names
- **Brushing** – sending unsolicited packages with QR codes
- **Card skimming** – surreptitiously reading chip cards

Typo-Squatting

5 Common Typosquatting Variations



Common Misspellings



Including www in the URL



Different Domain Suffixes



Adding an "S"



Adding Hyphens

4 Ways To Avoid Typosquatting Scams

Type Carefully, and Double-Check URLs Before Clicking



Look for the Lock

Don't Click on Links in Unsolicited Messages



Delete Suspicious Messages Immediately

Brushing Scam

 An Official website of the United States Government [Here's how you know](#)



UNITED STATES POSTAL
INSPECTION SERVICE

[ABOUT](#)

[CAREERS](#)

[TIPS & PREVENTION](#)

[NEWS](#)

[REPORT](#)



ALERT: IMPOSTER SCAMS CAN AFFECT ANYONE, AND OLDER AMERICANS ARE FREQUENTLY TARGETED. [LEARN MORE>](#)

Scam Article

Brushing Scam

Last updated 03.24.2025 | National

What could be better than opening the mailbox or the front door and finding an unexpected package? We all love surprises and gifts, but when these seemingly harmless free items come from a company or retailer, they may come with a higher cost than you realize. Oftentimes, this kind of unsolicited merchandise is part of a larger brushing scam, which is illegal in the U.S. and many other countries.

Card Skimming – ATM Swipe



Card Skimming – Contactless Chip

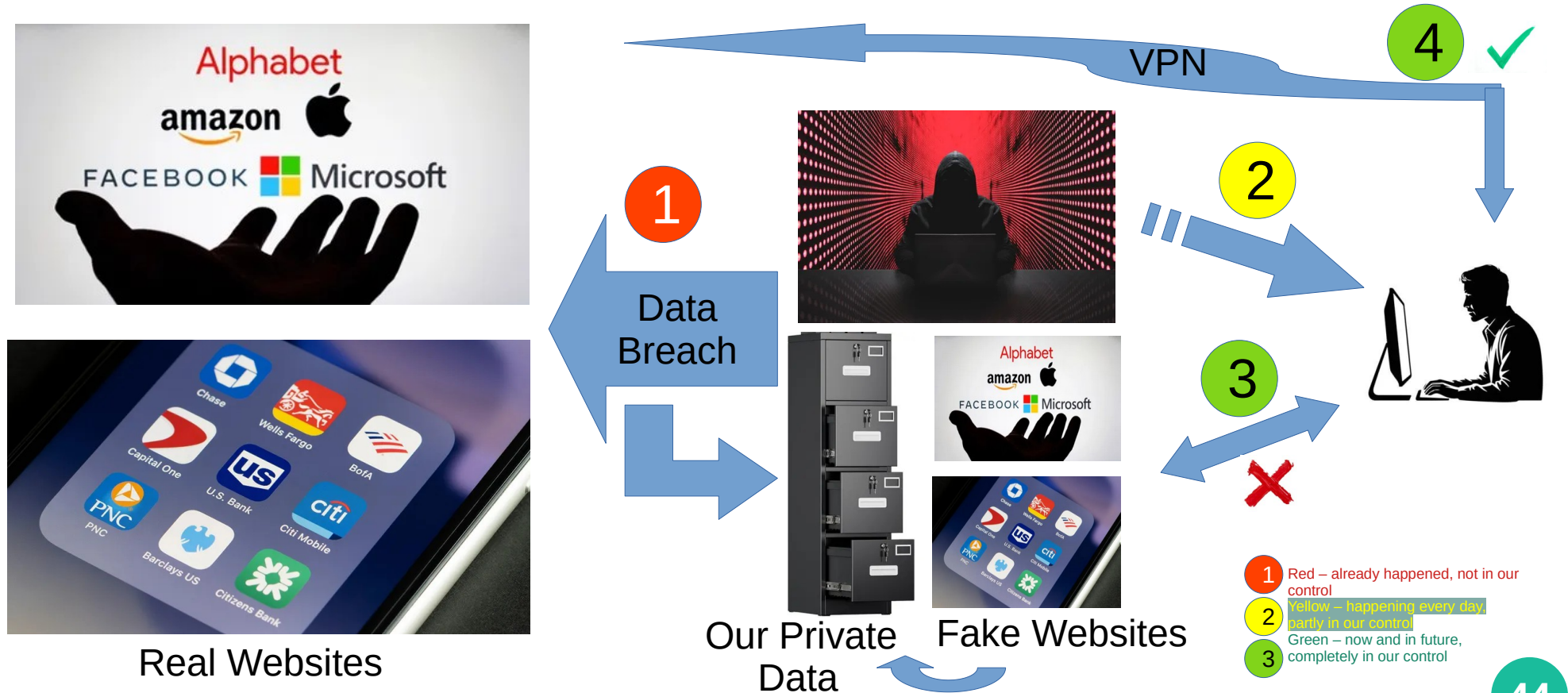
Unprotected Prox Cards Are Easy Targets



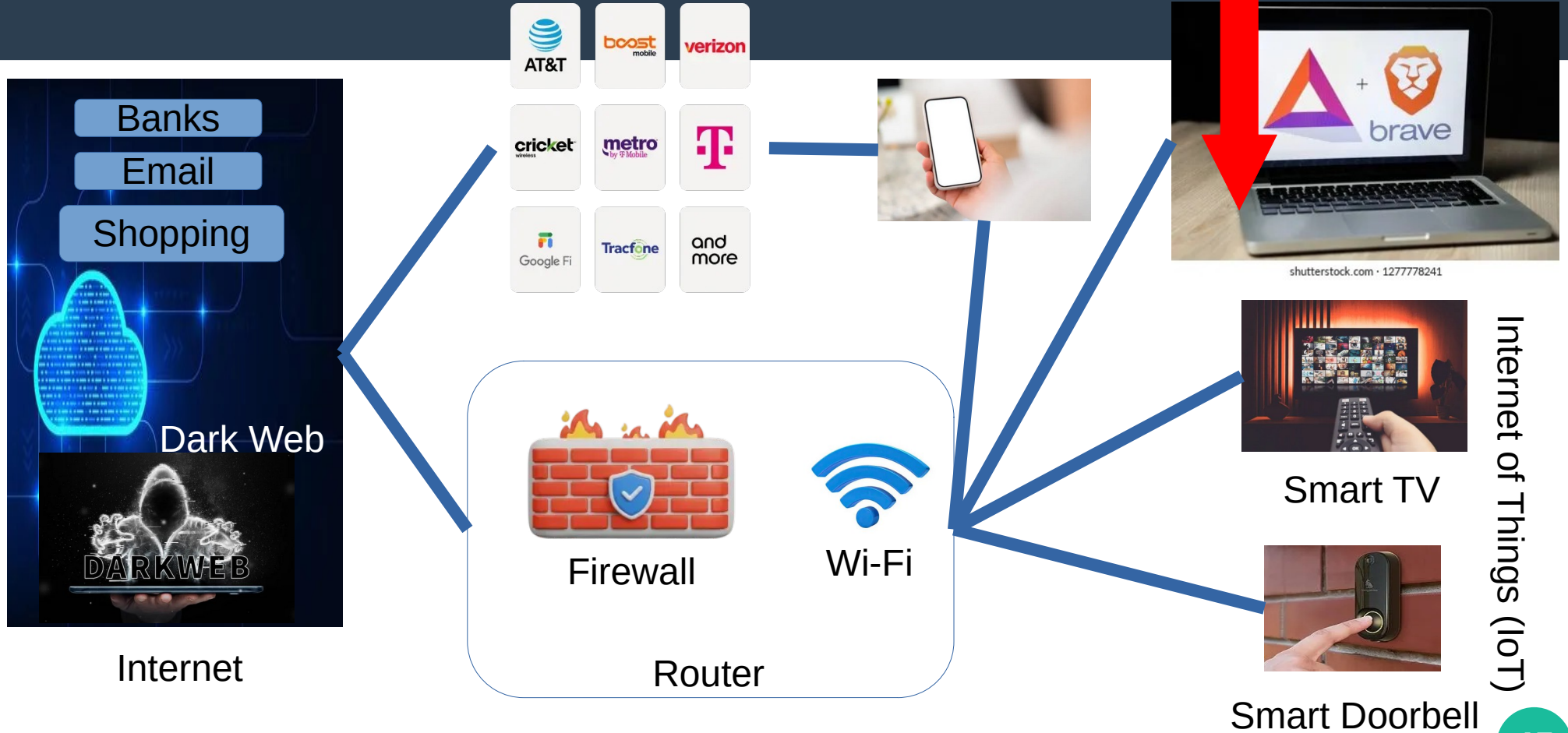
Card Skimming Prevention



Cyber-scam Life-cycle



The Big Picture



Computer/Laptop Security



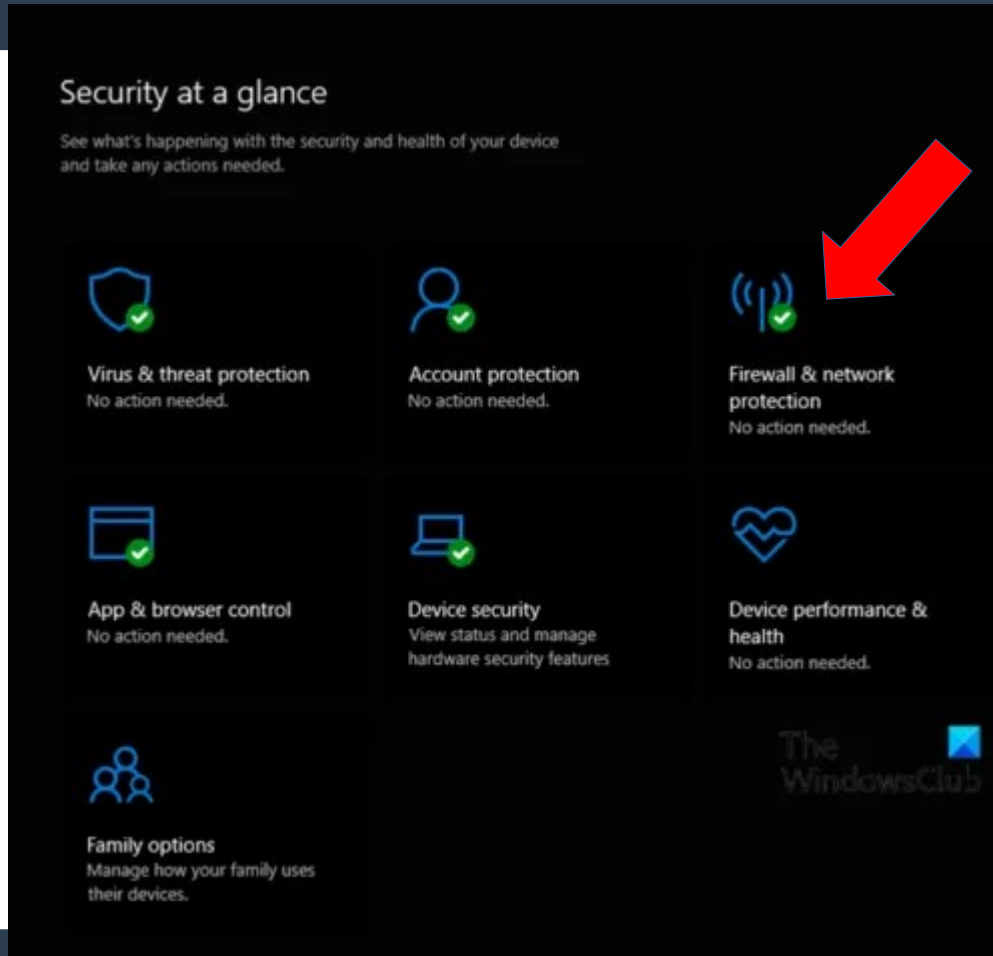
Computer - Components

- **Firewall (Ex: Windows Defender, if you use Windows)**
 - Blocks malicious Internet traffic from reaching into your computer
- **Anti-malware program (MalwareBytes, BitDefender, etc.)**
 - Detects and deletes any viruses, malware, spyware, adware
- **VPN**
 - Creates a secure pathway between your computer and the Internet

Computer - Components

- **Firewall (Ex: Windows Defender, if you use Windows)**
 - Blocks malicious Internet traffic from reaching into your computer
- **Anti-malware program (MalwareBytes, BitDefender, etc.)**
 - Detects and deletes any viruses, malware, spyware, adware
- **VPN**
 - Creates a secure pathway between your computer and the Internet

Microsoft Windows - Security Center



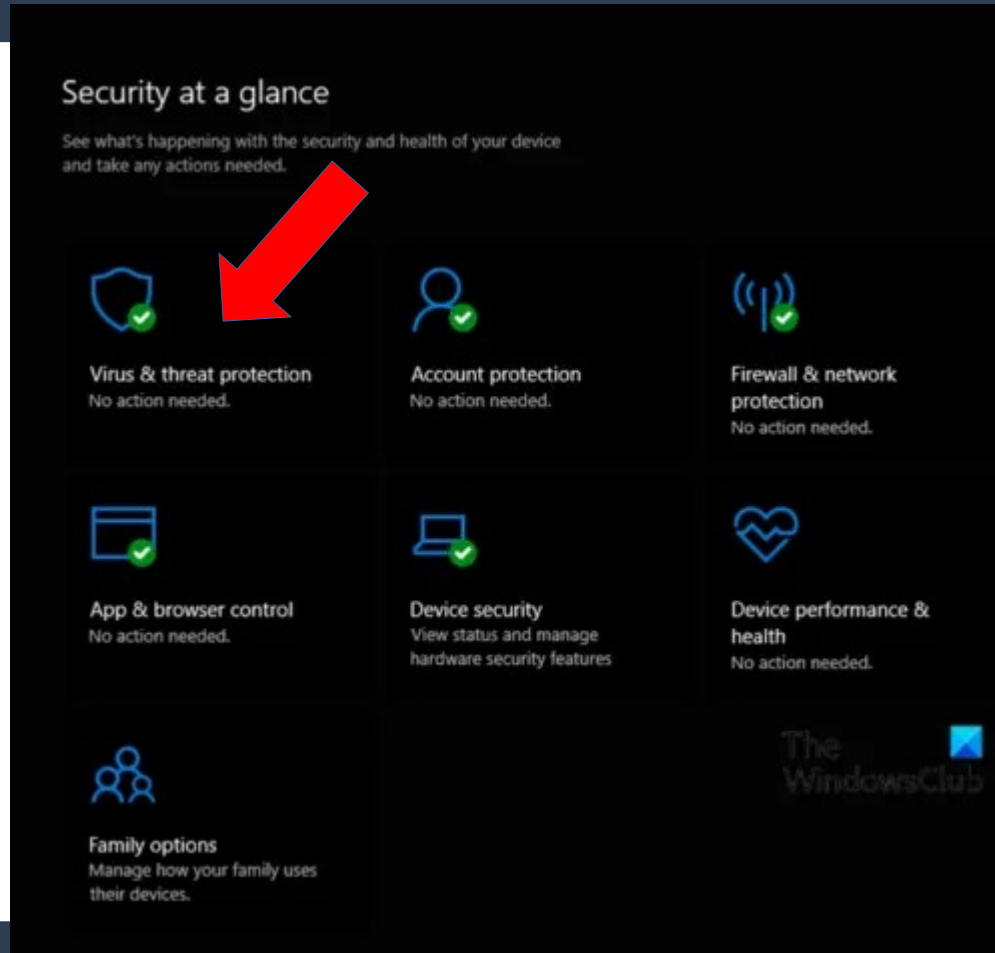
Mac OS - Firewall

- macOS includes a built-in application firewall that blocks unauthorized incoming connections, but it is **disabled by default** to prevent compatibility issues with services that don't listen on public internet ports. Enabling it adds a critical layer of security by preventing hackers from exploiting open ports or unprotected services, especially on public Wi-Fi
- **To turn on the firewall:**
 - Open System Settings and select Network.
 - Click Firewall and toggle the switch to On.
 - Click Options to configure advanced settings, such as Stealth Mode (hides your Mac from network scans) or allowing specific apps to receive incoming connections.

Computer - Components

- **Firewall (Ex: Windows Defender, if you use Windows)**
 - Blocks malicious Internet traffic from reaching into your computer
- **Anti-malware program (MalwareBytes, BitDefender, etc.)**
 - Detects and deletes any viruses, malware, spyware, adware
- **VPN**
 - Creates a secure pathway between your computer and the Internet

Operating System - Security Center



Mac OS - Anti-Malware

- While macOS includes built-in security features like Gatekeeper and App Review, they lack real-time malware scanning and advanced ransomware protection, making third-party antivirus software advisable for full safety

- The image shows a screenshot of the Macworld website. At the top is a blue navigation bar with the Macworld logo on the left and links for MAC, IPHONE, IPAD, APPLE WATCH, AIRPODS, VISION PRO, and MORE on the right. Below the navigation bar, the heading "At a glance" is centered. Underneath, there is a product recommendation for "Intego ONE". On the left is a small image of a laptop displaying the Intego software interface. To the right of the image, the text reads "Best antivirus for Mac users" in blue, followed by "Intego ONE" in black. Below this is a link "See why we picked it" with a downward arrow. To the right of the product name, it says "Best Price Today" in blue, followed by "\$29.99" in bold black, and "at Intego (annual)" in blue. On the far right is a blue button with the text "View Deal" in white.



#BestISPs

Best Products

Comparisons

Reviews

How-To

News

Deals

Newsletters



Maggie: AI Product Finder

PCMag editors select and review products independently. If you buy through affiliate links, we may earn commissions, which help support our testing.

Home > Best Products > Security > Antivirus

The Best Malware Removal and Protection Software for 2026

We've tested more than 100 anti-malware apps to help you find the best malware protection and removal software for all your devices.

OUR EXPERT



Neil J. Rubenking

Principal Writer, Security

Neil has covered cybersecurity for decades, testing the latest security apps against real-world threats to help you find the best protection.

LOOK INSIDE PC LABS

65

EXPERTS

44

YEARS

Edited By: Alan Henry

Updated April 6, 2026



Anti-Virus / Anti-Malware Software

CNET YOUR GUIDE
TO A BETTER FUTURE



News

AI

Tech

Home

Entertainment

Wellness

Gift Guides

Cover Stories

More

Tech > Antivirus > Services & Software

Best Antivirus 2026: A Tight Race, but Two Providers Lead the Pack



From premium companies like Bitdefender and Malwarebytes to budget tools like AVG, I've tested the most popular antivirus tools -- and found great options for keeping your devices safe.

OUR EXPERTS



Written by [Dianna Gunn](#)

Written by [Clifford Colby](#)

Written by [Attila Tomaschek](#)

• Article updated on April 16, 2026 at 5:35 PM PDT

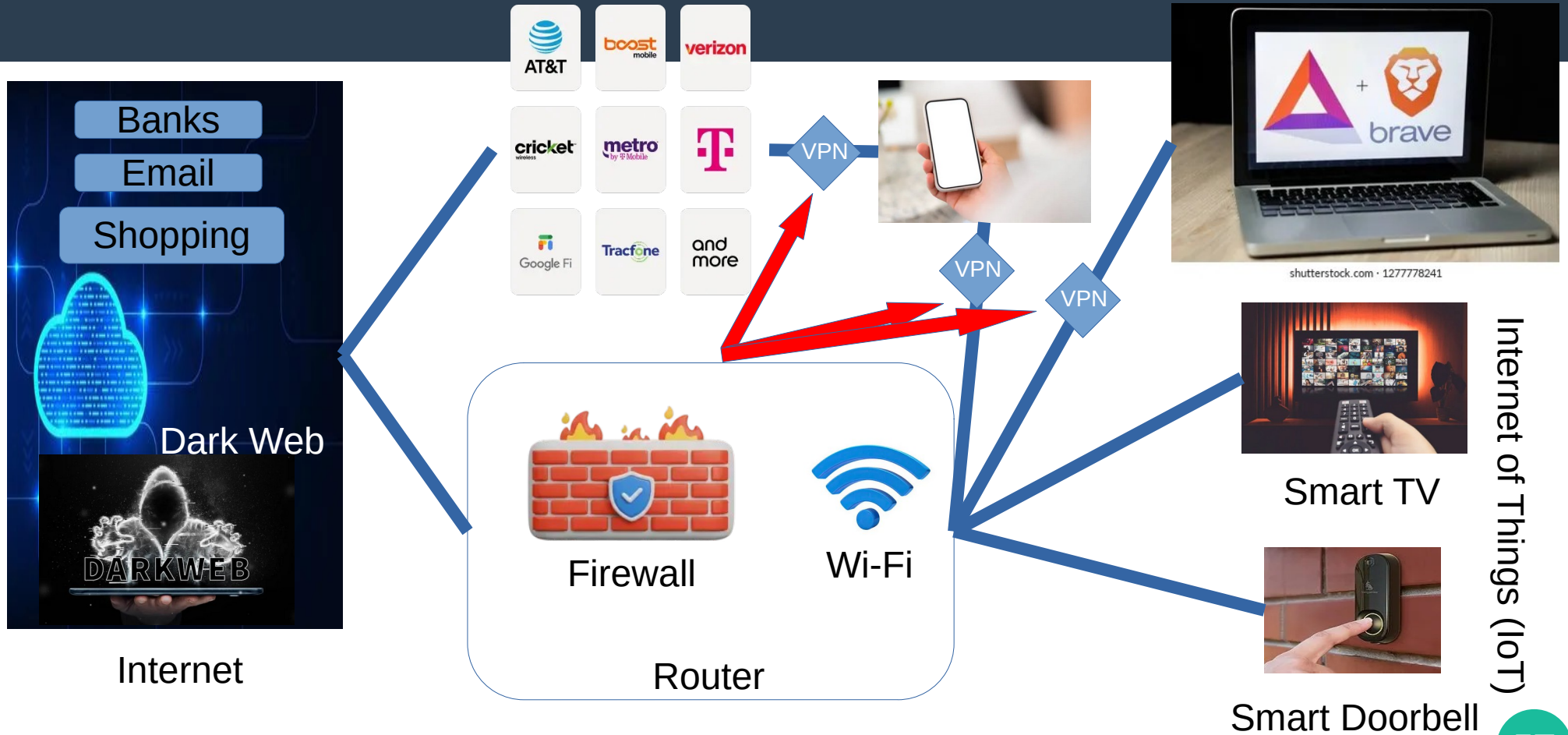
WHY YOU CAN TRUST CNET

Our devices contain important files for our careers, hobbies and personal connections. CNET's [latest antivirus survey](#) shows that over half (54%) of laptop owners have encountered potential malware on their personal laptop over the past 12 months. The best antivirus tools protect you by scanning files before you download them, as well as detecting [potential threats](#) already on your devices. While built-in antivirus protection on Windows and Mac computers can be solid, third-party antivirus options may give you nifty security benefits, like parental controls, scam detection and identity monitoring services. I retested our top antivirus picks in 2026 to assess their protection, performance and value to help you find the best antivirus for your needs.

Computer - Components

- **Firewall (Ex: Windows Defender, if you use Windows)**
 - Blocks malicious Internet traffic from reaching into your computer
- **Anti-malware program (MalwareBytes, BitDefender, etc.)**
 - Detects and deletes any viruses, malware, spyware, adware
- **VPN**
 - Creates a secure pathway between your computer and the Internet

The Big Picture



VPN (Virtual Private Network)

- **Virtual Private Networks (VPNs) create a secure connection by establishing an encrypted tunnel between your device and a remote server, masking your IP address and protecting data from interception on public networks**
- **Many VPN Providers also include anti-phishing and ad-blocking features**
- **Proton, Mullvad, NordVPN are some of the better ones**
- **Typically cost \$40 to \$80 an year**

The “Cybersafe Mindset”

- It's a process and a journey – not a one-and-done
- Rapid technological development = evolving threat landscape
- Yet, it has more to do with human psychology than technology
- Always remember it could be a scammer on the other end
- Entering and staying in the “cybersafe mindset”

Online Tools and Resources

- **Check out these websites**

- lakelandcybersafe.org
- securethevillage.org/cybersecurity-101-individuals

- **Government websites**

- opseniorshieldfl.com (Florida website for seniors, sign up for alerts)
- secureflorida.org (many resources for individuals and families)
- polksheriff.org/news-investigations/scam-reporting

Preview of Presentation 201

- **Privacy and how it relates to security**
- **Browsers and other apps on your computer and phone**
- **IP addresses and deep-dive into VPNs**
- **Computer operating system updates**
- **Smartphone privacy and security**
- **Smart TV privacy and security**
- **Introduction to Wi-Fi router security**

Thank you!

