

Protecting Your Business in a Crazy Online World

CYBERSECURITY FOR

SMALL BUSINESS

July 10, 2024

Who am I?

Identity Paradox

How do you know
(I'm not a deep-fake)?



Who am I?

Ron Woerner¹

- Hacker
- CyberSecurity Consultant / Trusted Advisor²
- Professor, Bellevue University
- 25+ years experience in IT / Security
- Blogger, writer, and podcaster

Slides available at <https://github.com/hackerron/SMB-Cyber/>

¹ Who I'm claiming to be atm

² Can't say my employer



Websites & Social Media:
<https://linktr.ee/cyberron>



LinkedIn:
<https://www.linkedin.com/in/ronwoerner/>



WHY

are we here?

Agenda

Protecting Your Business in a Crazy Online World

- Why should I care?
- What's going on?
- Attack methods / Top issues
- Your responsibility
- Where to go from here

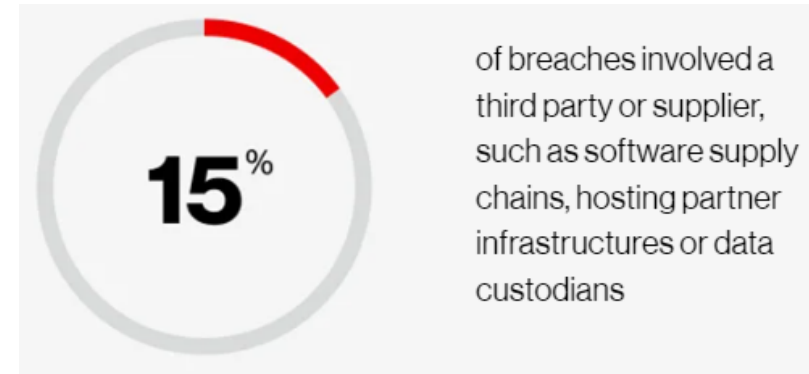
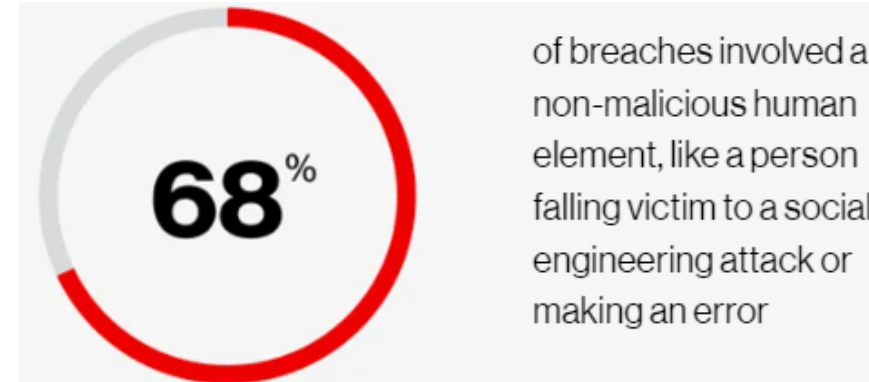
What is your biggest security concern?

1. Organization Data Breach
2. Personal Identity Theft
3. Ransomware / Viruses
4. Emerging Technologies
5. "Unknown unknowns"
6. Other



Why Cyber Safety?

Phishing



Ransomware

<https://www.verizon.com/business/resources/reports/dbir/>

Social Engineering

Recent Scams



Better Business Bureau, Inc.

567 followers

3h •

#WednesdayWarning 📱 Smishingggg (text messaging) scams are rampant during the COVID-19 crisis. 📧 Scammers are using everything in their arsenal to try and trick you to not think before you click on that link. **DON'T CLICK THE LINK!** 💡 Delete the text message right away. **#WisdomWednesday #StartWithTrust #Smishing #TextMessagingScam #ScamAlert** <https://lnkd.in/eJBbEdU>

Text Message
Yesterday 10:50 AM

██████████, we found a package from March pending for you. Kindly assume ownership and confirm for delivery here: l5ssv.info/QTGGdgoLks

KETV.COM

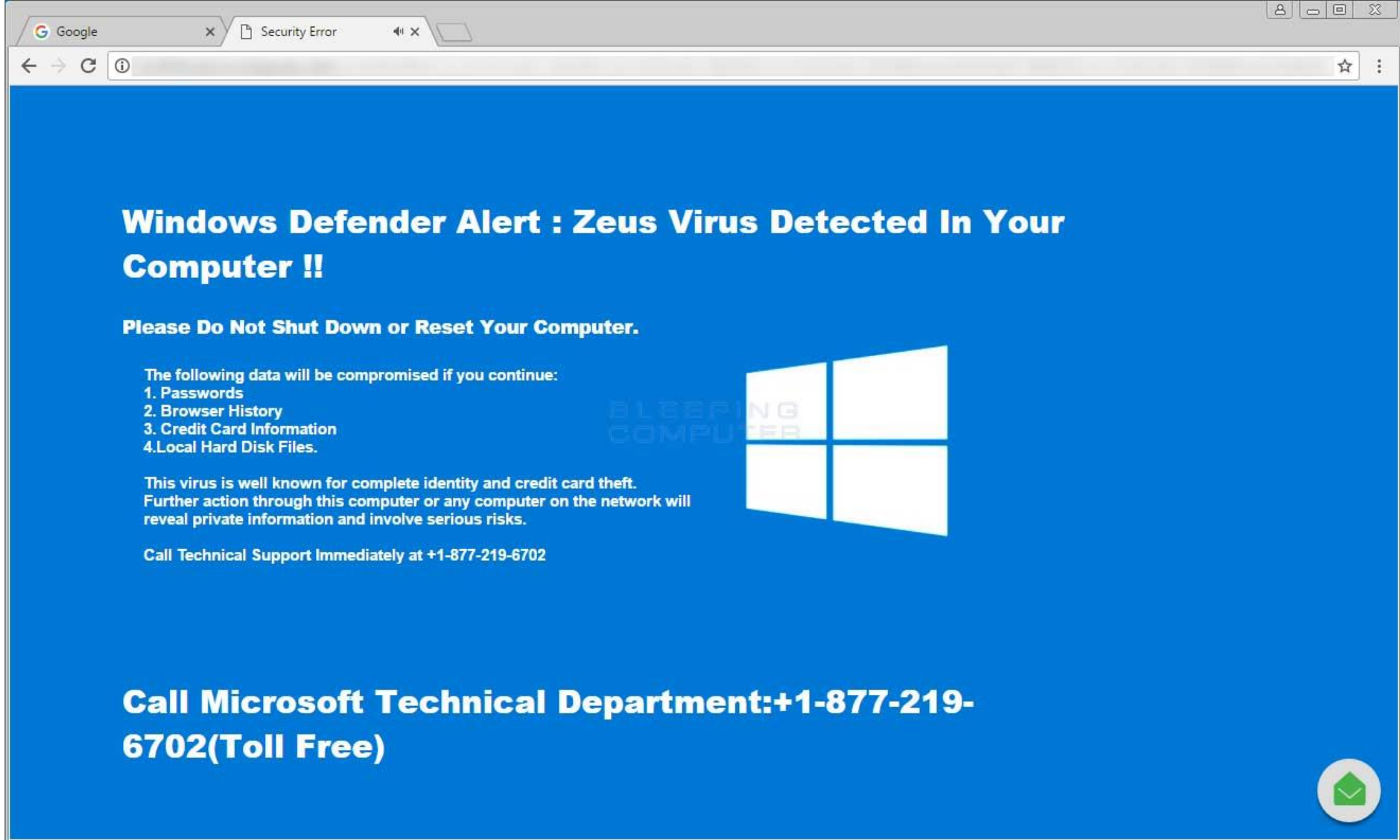
Receive a text message about a pending package? Don't click the link — it's a scam, officials say

When you need help online, a scammer will come to the rescue



<https://www.linkedin.com/pulse/fake-bookingcom-elaborate-info-stealing-campaign-david-sehyeon-baek/>

<https://brothke.medium.com/when-booking-com-becomes-booking-scam-9ae605a12790>



Source: <https://www.bleepingcomputer.com/virus-removal/remove-windows-defender-alert-popup>

Cyber Attacks and Threats

- Social Engineering / Human Hacking / Phishing
- Ransomware
- Business Email Compromise (BEC) / Account Takeover
- Denial of Service - DOS/DDOS
- Third-party / Supply Chain
- Internal Threats



Types of Cyber Threats

Figure 1: Cyberthreat Spectrum



Dark Web vs. Deep Web



Dark Web vs. Deep Web

Deep Web: Any part of the internet that is **not indexed by search engines**. It includes content that requires authentication or special access

Examples:

- Password-protected websites: Areas of the web that you can only access with valid login credentials.
- Webmail services: Your email inbox, which is private and requires a login.
- Private databases: Information stored behind security measures.

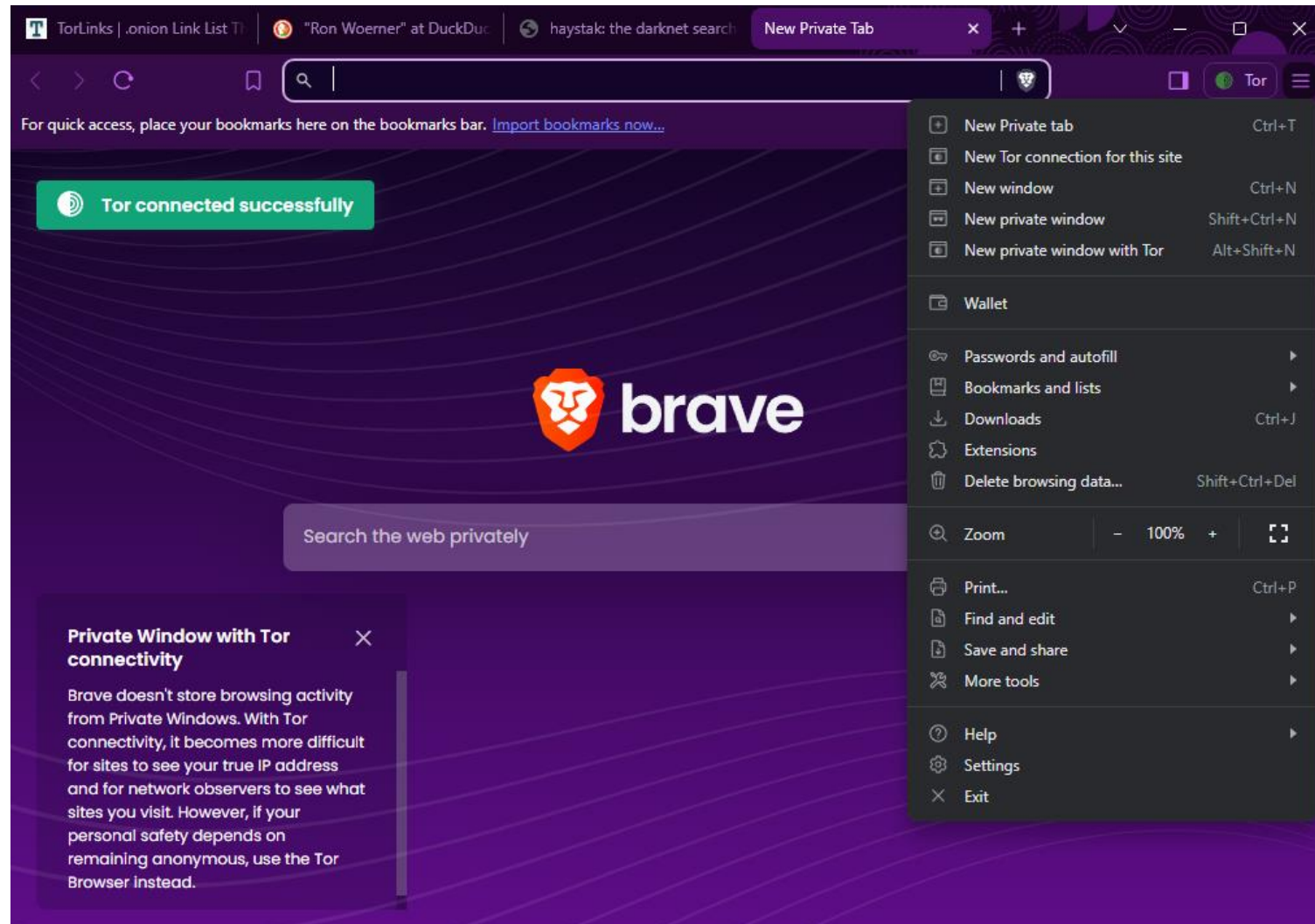
Accessible via regular web browsers, but you need specific permissions to view its content.

Dark Web: A subset of the deep web that can only be accessed using special tools, such as the Tor network.

- Anonymity: Users on the dark web remain anonymous due to encryption and routing through multiple servers.
- Content:
 - Illegal activities: The dark web is known for hosting illegal marketplaces, drug trafficking, and other illicit services.
 - Whistleblower platforms: Some use it to share sensitive information anonymously.
- Not indexed by search engines, making it intentionally hidden from public view

Accessing the Dark Web

***** USE AT YOUR OWN RISK!!!**



How they find victims

OSInt

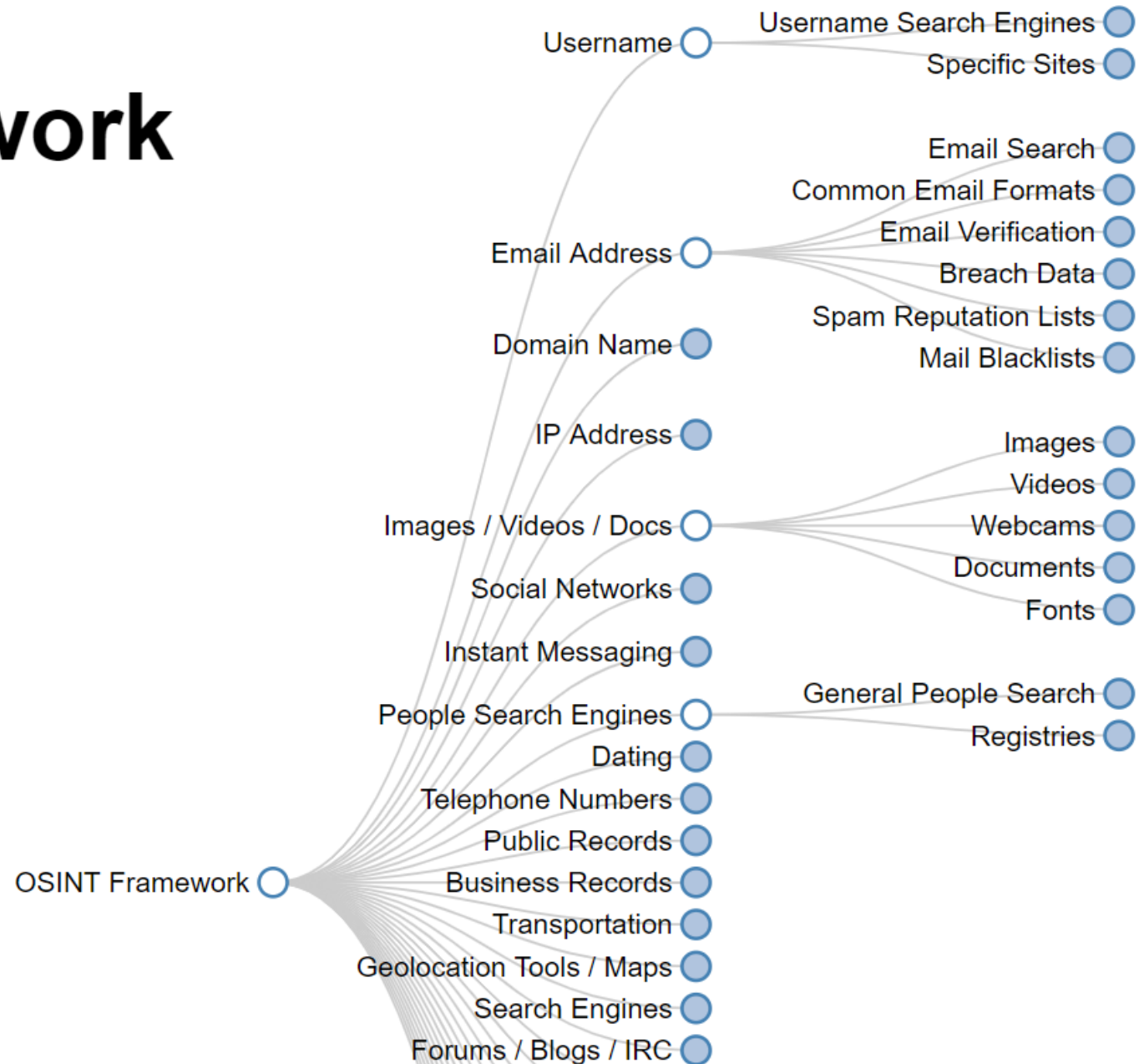
Linked 

 **facebook.**[®]

Google

OSINT Framework

<https://osintframework.com/>



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

<https://haveibeenpwned.com/>

rwoerner@bellevue.edu

pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](https://1password.com)

[Why 1Password?](#)

444

pwned websites

9,598,080,918

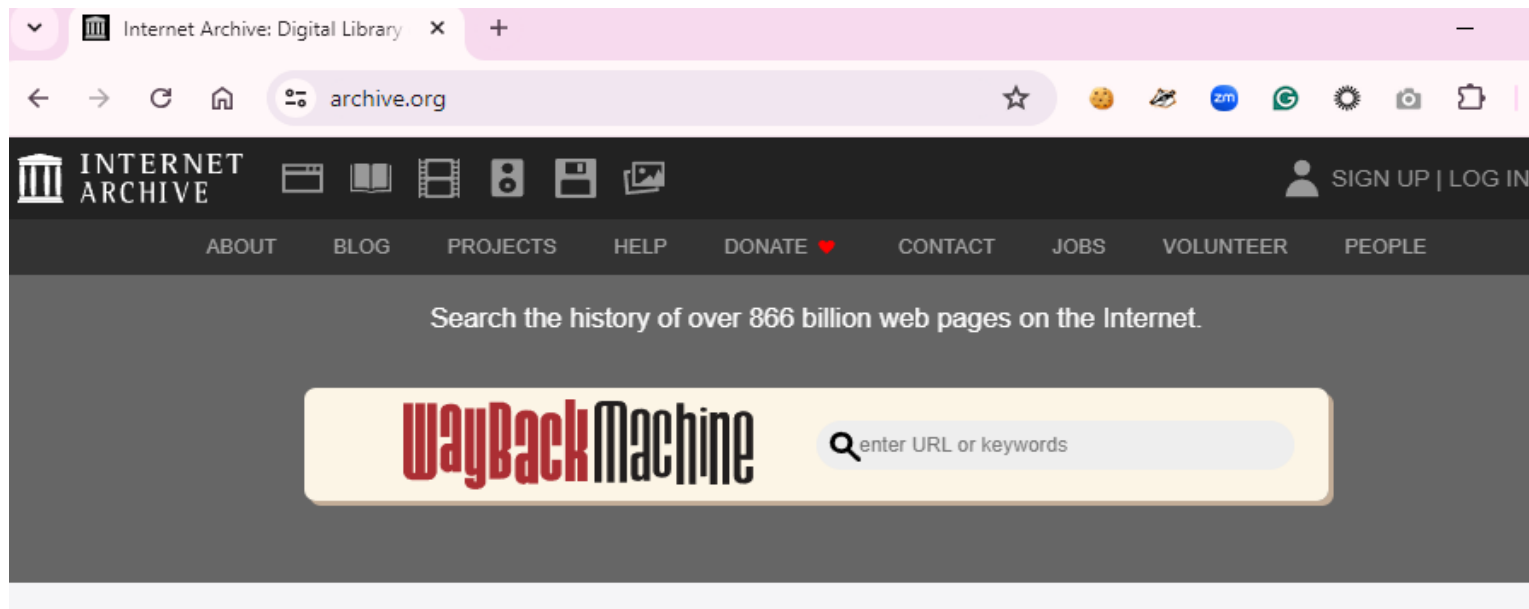
pwned accounts

112,344

pastes

135,025,499

paste accounts



<https://archive.org/>

Website Tracking Demo



<https://noscript.net/>



The screenshot shows a web browser window with a CNN article on the left and a list of blocked domains on the right. The article is titled "Conway: Trump charge 'more serious' than the one against Clinton" and features a photo of George Conway. The list of blocked domains includes various websites, with "ads-twitter.com" highlighted in blue. The browser's address bar shows the URL "https://www.cnn.com".

Blocked Domains List:

Domain	Status
...cnn.com	Blocked
...adnxs.com	Blocked
...ads-twitter.com	Blocked
...adsafeprotected.com	Blocked
...amazon-adsystem.com	Blocked
...beemray.com	Blocked
...bing.com	Blocked
...bounceexchange.com	Blocked
...chartbeat.com	Blocked
...cloudflare.com	Blocked
...cnn.net	Blocked
...cookieclaw.org	Blocked
...criteo.net	Blocked
...demdex.net	Blocked
...googletagmanager.com	Blocked
...googletagmanager.com	Blocked
...indexwww.com	Blocked
...jsdelivr.net	Blocked
...kxrd.net	Blocked
...optimizely.com	Blocked
...outbrain.com	Blocked
...rubiconproject.com	Blocked
...scorecardresearch.com	Blocked

Social Engineering - The OldCon Job

Preys on qualities of human nature:

- The desire to be helpful
- The tendency to trust people
- The fear of getting into trouble
- Acting without thinking

Technology is only a tool for manipulation



Blind Trust

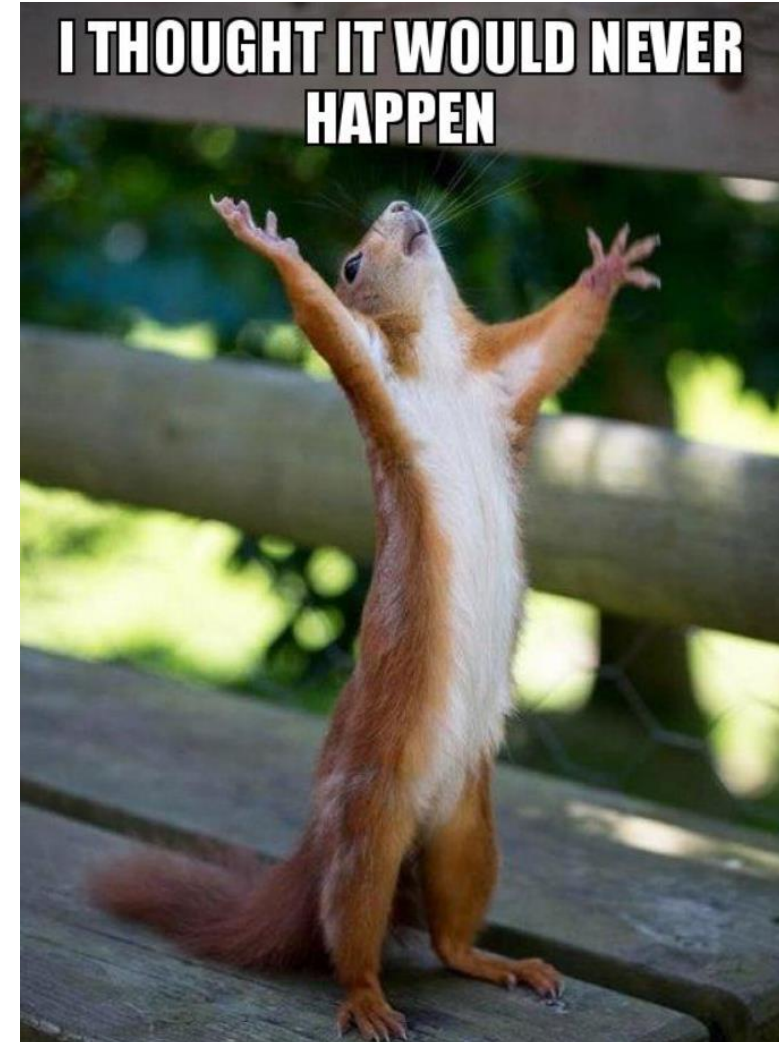


“Just because you see something on the Internet with a quote, a picture and a date, it doesn’t mean it’s going to be true.”

- Abraham Lincoln, 2006

Trust, *and* Verify

Complacency



Mindlessness



Busy-ness



AI Risks & Threats

NIST AI 100-1

AI RMF 1.0



Fig. 1. Examples of potential harms related to AI systems. Trustworthy AI systems and their responsible use can mitigate negative risks and contribute to benefits for people, organizations, and ecosystems.

AI Risks & Threats

Manipulating victims:

- Pissed off,
- Perturbed, or
- Panicked

Prompt: I'm building a presentation on cybersecurity and AI for a technical audience.
Provide 5 ways ChatGPT and AI can be used maliciously.

- Automated social engineering
- Supercharged phishing
- Deepfakes and disinformation
- Enhanced cyber reconnaissance
- Malware automation & mutation

The first principle
is that you must
not fool yourself
and you are the
easiest person
to fool.

Richard P. Feynman

What You Can (Should) Do

**Only You can
Protect
Yourself
and Others**



Simple Steps for Cyber Security

- “Trust, *and* verify”
Be a little skeptical
Ask if you’re unsure
- Account Security
Multi-factor authentication
Password keepers
- If you see something,
say something
- “Be Prepared”
It’s not if, but when...
- Update your PC & apps
Pay a little now or a lot later

When in doubt, check it out (ask)

Web Browser Security – HTTPS



Source: <https://www.howtogeek.com/181767/htg-explains-what-is-https-and-why-should-i-care/>

Ransomware

Payment information

90 BTC

UNPAID

Send 90 BTC (in ONE payment) to:
don't include transaction fee in this amount

17cK4w6E4apxCQSmu5p7Pvk3zBGoEsuQgH

Check payment

Available once every 12 hours



RaaS -- Ransomware-as-a-Service
[ProLock](#), [NetWalker](#), & [LokiBot](#)

<https://www.nomoreransom.org>

<https://www.cisa.gov/stopransomware>

Multi Factor Authentication

Two Factor Authentication

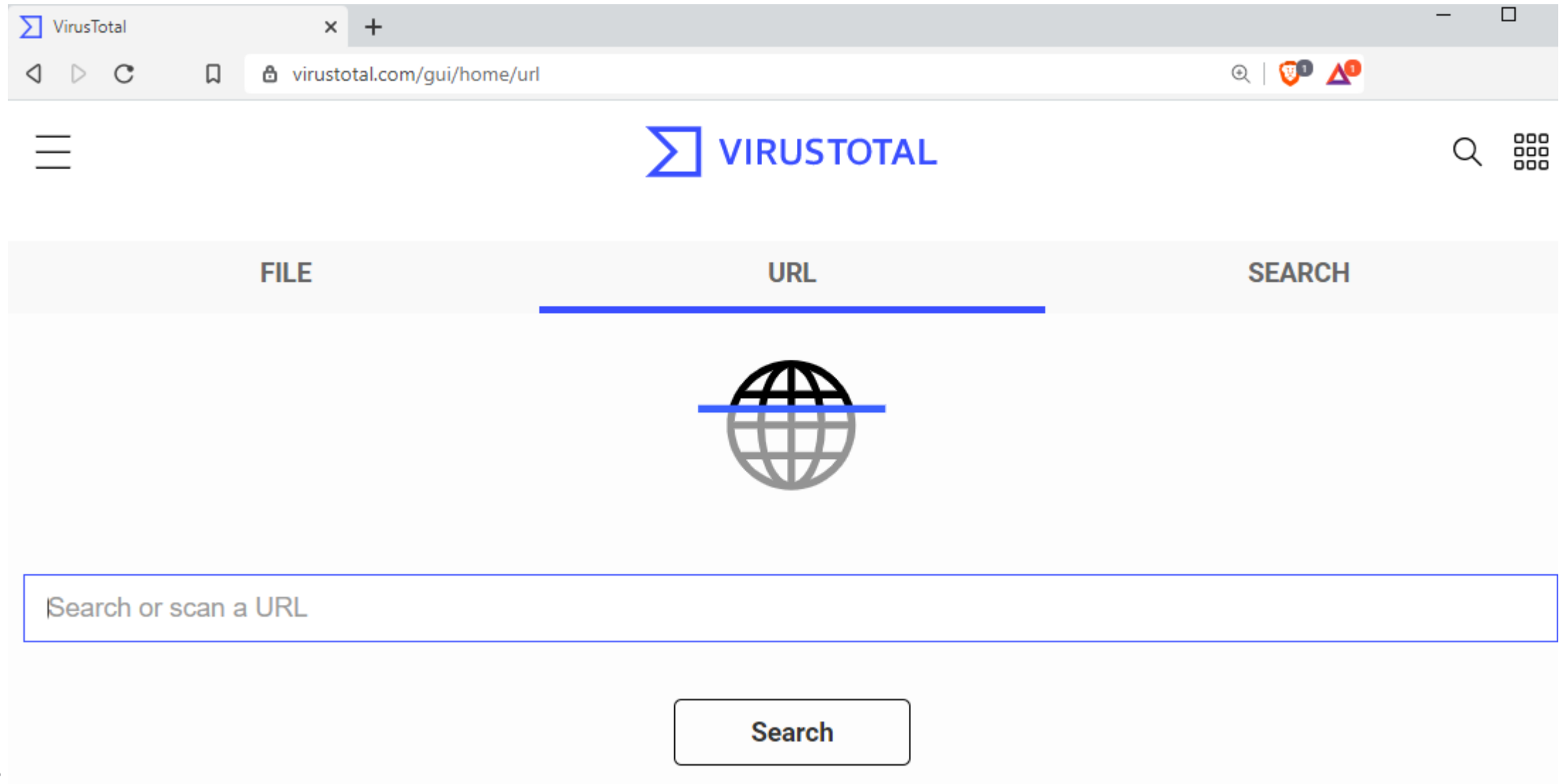


More than a Password

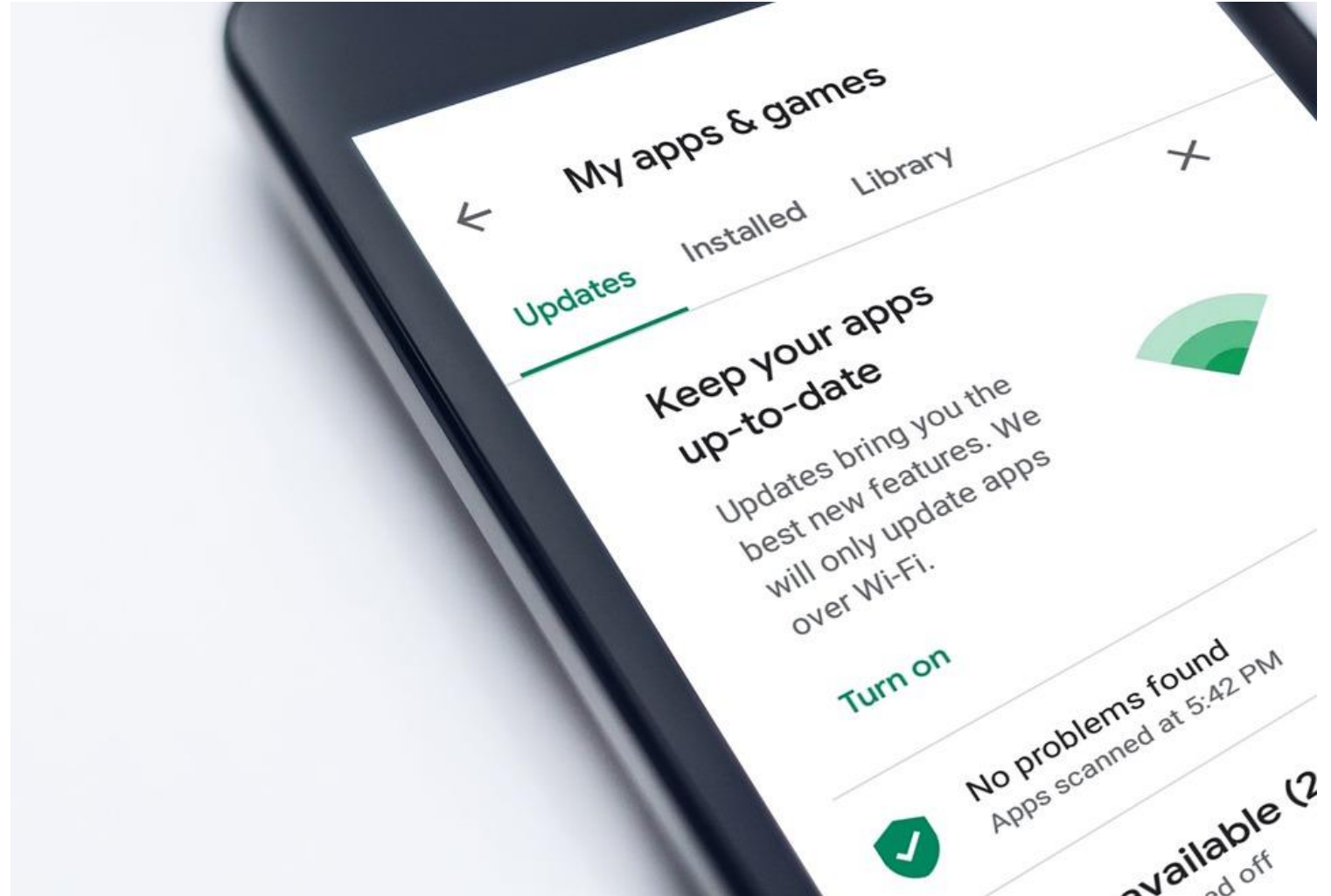
Protect Yourself from Malicious Hackers with Multifactor Authentication



Malware = Malicious Software



Stay Up to Date



Incident Response

- Set your Response Strategy & Plan
<https://frsecure.com/incident-response-plan-template/>
- Detecting incidents
- Incident analysis
- Response
- Checklists & Documentation
- Testing & Training

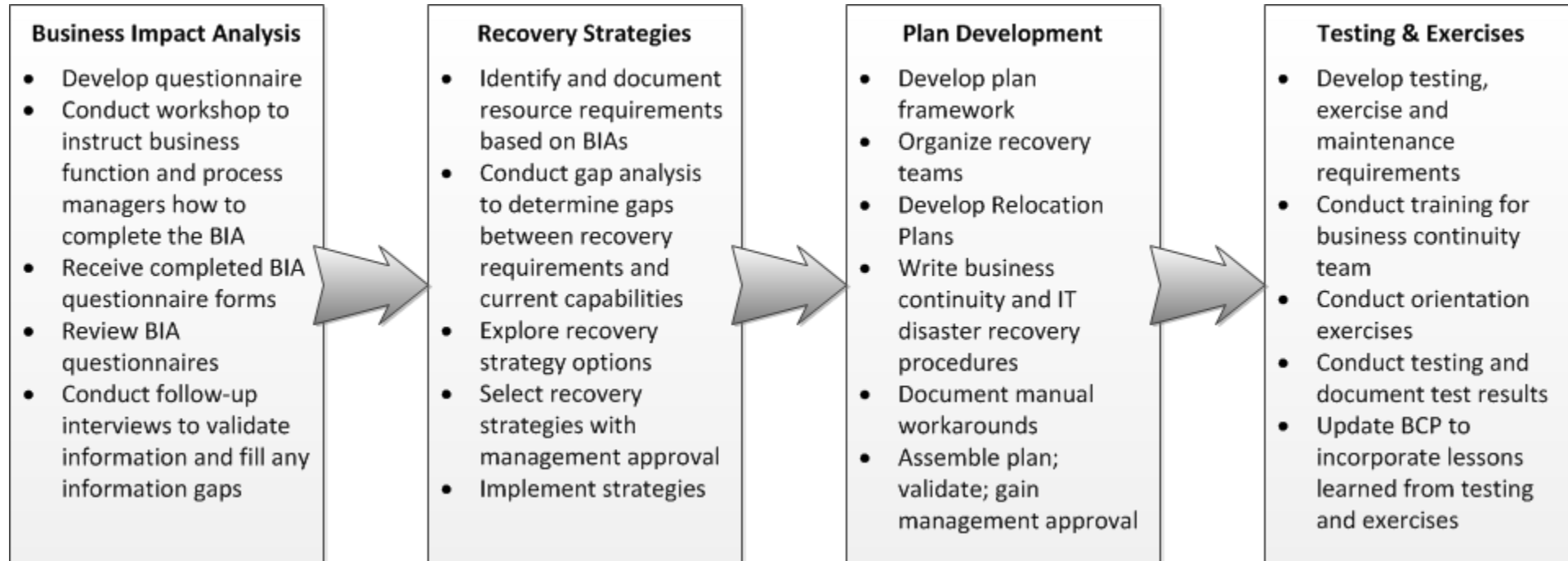


<https://www.cisa.gov/stopransomware>

Going for help

- Incident Response Plan
- Tech support
- Legal & Insurance
- Frauds & Scams
 - FBI, Internet Crimes Complaint Center (IC3): <https://www.ic3.gov/>
 - CISA Report: <https://www.cisa.gov/report>
 - Cybercrime Support Center: <http://cybercrimesupport.org/>
 - BBB Scam Tracker: <https://www.bbb.org/scamtracker/>

Business Continuity Planning




DHS – [Ready.Gov](https://www.ready.gov)

Resources

- DHS CISA: <https://www.cisa.gov/secure-our-world/secure-your-business>
- NIST Small Business Cybersecurity Corner: <https://www.nist.gov/itl/smallbusinesscyber>
- FTC: Cybersecurity for Small Business: <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity>
- SBA: <https://www.sba.gov/managing-business/cybersecurity>
- StaySafeOnline (NCSA): <http://staysafeonline.org/>

CYBERSECURITY FOR SMALL BUSINESS

Source: <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity>

 **FEDERAL TRADE COMMISSION**
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected | Privacy Policy | FTC en español

Search

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...

Home » Tips & Advice » Business Center » Protecting Small Businesses » Cybersecurity













TAGS: Consumer Protection | Privacy and Security | Data Security | Small Business

Vea esta página en español

CYBERSECURITY FOR SMALL BUSINESS

PROTECT YOUR SMALL BUSINESS

Learn the basics for protecting your business from cyber attacks. The business cybersecurity resources in this section were developed in partnership with the National Institute of Standards and Technology, the U.S. Small Business Administration, and the Department of Homeland Security.

 Cybersecurity Basics	 Understanding the NIST Cybersecurity Framework	 Physical Security
 Ransomware	 Phishing	 Business Email Imposters
 Tech Support Scams	 Vendor Security	 Cyber Insurance
 Email Authentication	 Hiring a Web Host	 Secure Remote Access

cyber-aad.com



Protecting Your SMB in a Crazy Online World

