Phishing, Pharming, Smishing, and Other Cyberattacks that Can Ruin a Lawyer's Career

Tips, Tools, and Techniques for Protecting Your Firm

Honorable Judge Mary Evans, Esq.
Mira White, Esq. B.C.S., CPA
Jeffrey Rapkin, Esq.
Michael Shemkus, Esq.

TOPICS

* HOW IS THIS HAPPENING? (IOT!!!!!!!!!)
* ATTORNEYS UNDER ATTACK, SPECIFIC EXAMPLES
* LATEST SCAMS AND TECHNIQUES BEING UTILIZED: RANSOM, PHISHING, PHARMING, SMISHING, SOCIAL MEDIA, GRANDPARENT SCAM, DATING, "OFFERS," SPOOFING, ETC.
* WHY (AND HOW THESE TECHNIQUES WORK)
* HOW TO PROTECT YOURSELF: BACKUPS, VIRUS PROTECTION PROGRAMS, WHAT TO DO IF ATTACKED WITH RANSOMWARE OR OTHER MALWARE, VPNS, ETC.
* DON'T BE A VICTIM OF SOCIAL ENGINEERING
* TIPS, TOOLS, TECHNIQUES

AS LAWYERS, WE HAVE AN ENDURING ETHICAL OBLIGATION TO PROTECT OUR CLIENT'S PRIVATE INFORMATION.

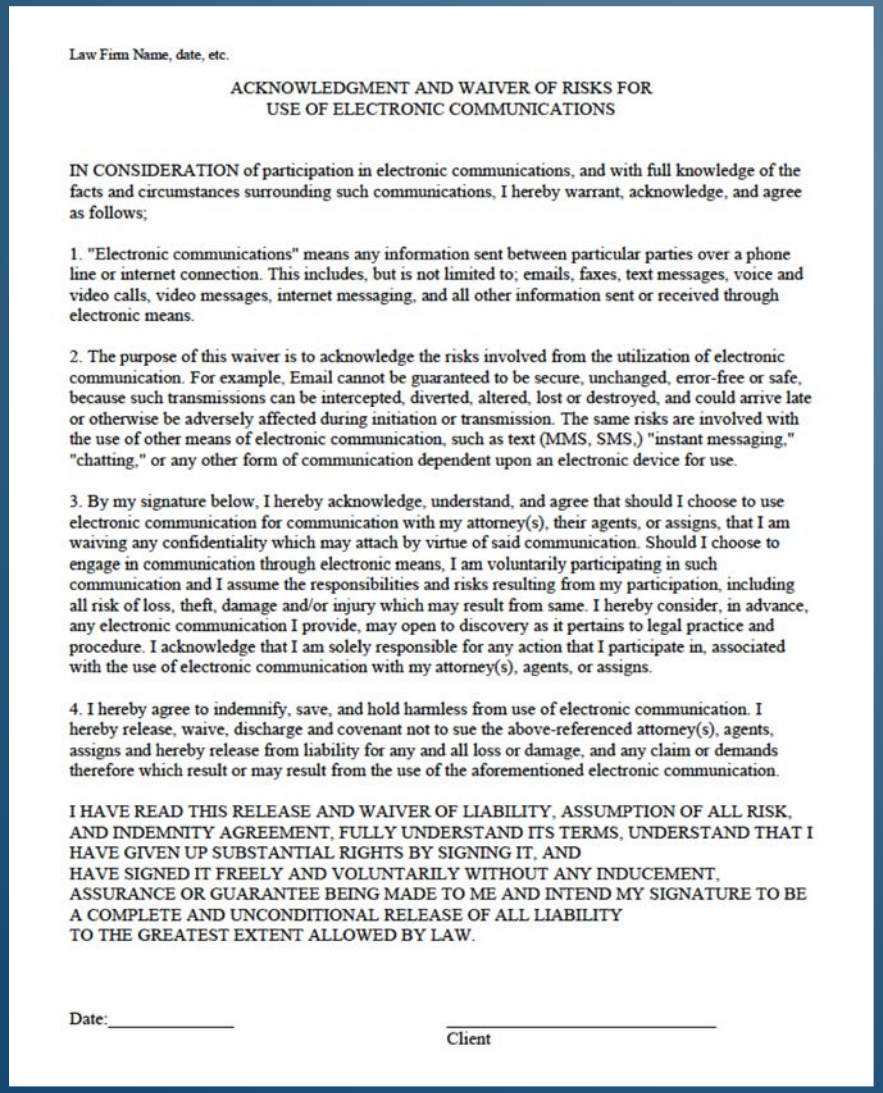
Getting hacked could mean the end of a lawyer's career.

We are being listened to. We are being tracked.

We are being hacked.

Protect yourself. Protect your clients.


LAW & CRIME CHANNEL
ALEX JONES TRIAL FROM EARLIER TODAY
SANDY HOOK 'HOAX' LAWSUIT DEFAMATION CIVIL TRIAL
TDS
TREVOR NOAH



Law Firm Name, date, etc.

ACKNOWLEDGMENT AND WAIVER OF RISKS FOR
USE OF ELECTRONIC COMMUNICATIONS

IN CONSIDERATION of participation in electronic communications, and with full knowledge of the facts and circumstances surrounding such communications, I hereby warrant, acknowledge, and agree as follows;

1. "Electronic communications" means any information sent between particular parties over a phone line or internet connection. This includes, but is not limited to; emails, faxes, text messages, voice and video calls, video messages, internet messaging, and all other information sent or received through electronic means.

2. The purpose of this waiver is to acknowledge the risks involved from the utilization of electronic communication. For example, Email cannot be guaranteed to be secure, unchanged, error-free or safe, because such transmissions can be intercepted, diverted, altered, lost or destroyed, and could arrive late or otherwise be adversely affected during initiation or transmission. The same risks are involved with the use of other means of electronic communication, such as text (MMS, SMS,) "instant messaging," "chatting," or any other form of communication dependent upon an electronic device for use.

3. By my signature below, I hereby acknowledge, understand, and agree that should I choose to use electronic communication for communication with my attorney(s), their agents, or assigns, that I am waiving any confidentiality which may attach by virtue of said communication. Should I choose to engage in communication through electronic means, I am voluntarily participating in such communication and I assume the responsibilities and risks resulting from my participation, including all risk of loss, theft, damage and/or injury which may result from same. I hereby consider, in advance, any electronic communication I provide, may open to discovery as it pertains to legal practice and procedure. I acknowledge that I am solely responsible for any action that I participate in, associated with the use of electronic communication with my attorney(s), agents, or assigns.

4. I hereby agree to indemnify, save, and hold harmless from use of electronic communication. I hereby release, waive, discharge and covenant not to sue the above-referenced attorney(s), agents, assigns and hereby release from liability for any and all loss or damage, and any claim or demands therefore which result or may result from the use of the aforementioned electronic communication.

I HAVE READ THIS RELEASE AND WAIVER OF LIABILITY, ASSUMPTION OF ALL RISK, AND INDEMNITY AGREEMENT, FULLY UNDERSTAND ITS TERMS, UNDERSTAND THAT I HAVE GIVEN UP SUBSTANTIAL RIGHTS BY SIGNING IT, AND
HAVE SIGNED IT FREELY AND VOLUNTARILY WITHOUT ANY INDUCEMENT, ASSURANCE OR GUARANTEE BEING MADE TO ME AND INTEND MY SIGNATURE TO BE A COMPLETE AND UNCONDITIONAL RELEASE OF ALL LIABILITY
TO THE GREATEST EXTENT ALLOWED BY LAW.

Date:_____ _____
Client

You might be able to improve this. If you do, please share with the rest of us. A hard copy is in the materials provided, but you can download a copy in MS Word at:

https://www.rapkinlegal.com/emailclass

ETHICAL CONSIDERATIONS

4-1. CLIENT-LAWYER RELATIONSHIP RULE 4-1.1 COMPETENCE

A lawyer must provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

Maintaining competence

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education, including an understanding of the benefits and risks associated with the use of technology, and comply with all continuing legal education requirements to which the lawyer is subject.

RULE 4-1.6 CONFIDENTIALITY OF INFORMATION

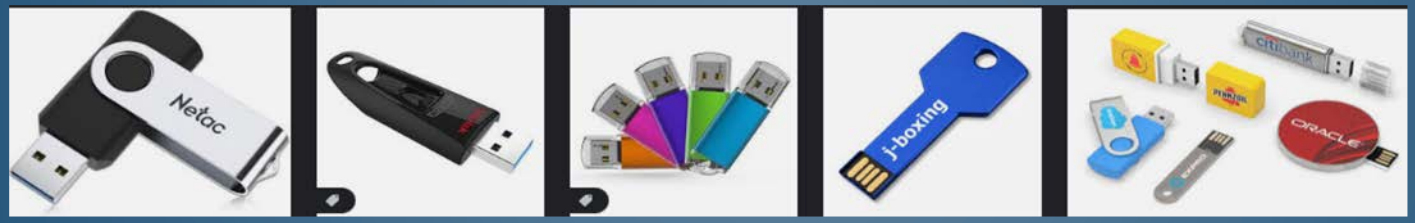
(e) Inadvertent Disclosure of Information. A lawyer must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Acting Competently to Preserve Confidentiality

Paragraph (e) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See rules 4- 1.1, 4-5.1 and 4-5.3.

RULE 4-1.18 DUTIES TO PROSPECTIVE CLIENT

GOT ANY OF THESE LYING AROUND????



PROPER DISPOSAL IS AN ETHICAL OBLIGATION.

FLORIDA BAR ETHICS OPINION
OPINION 10-2
September 24, 2010

Advisory ethics opinions are not binding.

A lawyer who chooses to use Devices that contain Storage Media such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition, including: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

FLORIDA BAR ETHICS OPINION
OPINION 21-1
June 10, 2021

Advisory ethics opinions are not binding.

A lawyer may not disclose information concerning a client's representation without the client's informed consent when responding to negative online reviews posted by individuals who are not current clients or former clients. If accurate, the lawyer may state that the person who made the post is not a current client or former client. The lawyer may generally note that the comments in the review are inaccurate but that the lawyer's response is constrained by the lawyer's ethical obligations.

ONLINE COMMENTS…

FLORIDA BAR ETHICS OPINION
OPINION 20-01
October 9, 2020

Advisory ethics opinions are not binding.

A lawyer may not disclose information relating to a client's representation in response to a negative online review, but may respond with a general statement that the lawyer is not permitted to respond as the lawyer would wish, but that the online review is neither fair nor accurate.

RESPONSE TO NEGATIVE ONLINE COMMENTS…

FLORIDA BAR ETHICS OPINION
OPINION 07-1
September 7, 2007

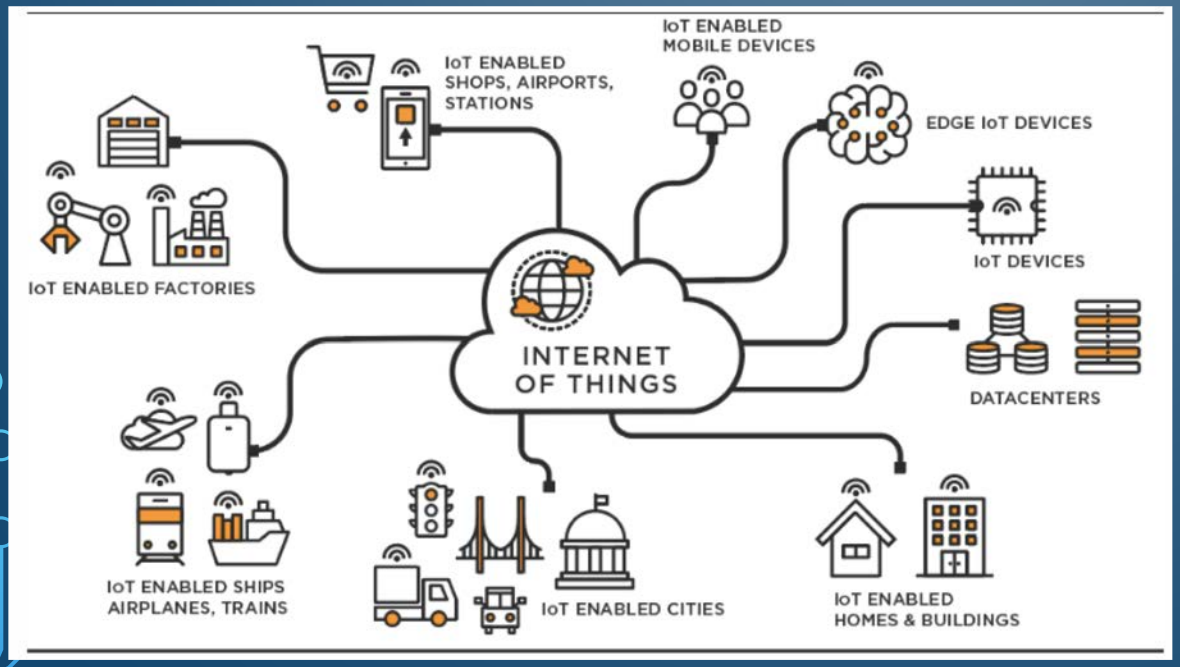
Advisory ethics opinions are not binding.

A lawyer whose client has provided the lawyer with documents that were wrongfully obtained by the client may need to consult with a criminal defense lawyer to determine if the client has committed a crime. The lawyer must advise the client that the materials cannot be retained, reviewed or used without informing the opposing party that the inquiring attorney and client have the documents at issue. If the client refuses to consent to disclosure, the inquiring attorney must withdraw from the representation.

WRONGFULLY OBTAINED INFORMATION…

HERE IS THE PROBLEM NO ONE IS TELLING YOU ABOUT: IT'S CALLED "THE INTERNET OF THINGS."

The "Internet of Things," (IOT), gathers information which seems harmless. But if you swore an oath to protect your clients' information, and your home is littered with listening devices, you may have a problem…



IT STARTS WITH INFORMATION GATHERING.

Introducing “the internet of things.” (IOT) If it’s connected to the internet, it can be accessed and hacked.

Introducing “the internet of things.” (IOT) If it’s connected to the internet, it can be accessed and hacked.

SMART DEVICES

Smart Toaster

Smart toast? Really? What happens when Skynet gets control of my toaster? This is Armageddon.

Smart Refrigerator, Smart Stove, Smart Washer and Dryer, Smart Microwave, Smart Toothbrush

Data collection may not be an issue for non-lawyers.

SMART FORK, SMART CAT FEEDER, SMART OVULATION DEVICE

Introducing "the internet of things." (IOT) If it's connected to the internet, it can be accessed and hacked.

If a device is "smart," it is connected to the internet. Smart devices collect data about your life. (What about passwords?)

THE DEVICES TALK TO ONE ANOTHER.

They use software called “APIs” to communicate.

An Application Programming Interface (API) is a software connection that allows applications to communicate and share services. In contrast to a user interface, which connects a computer to a person, an application programming interface connects computers or pieces of software to **each other.**

Introducing “the internet of things.” (IOT) If it’s connected to the internet, it can be accessed and hacked.

SMART-TOASTERS ARE EASY TO HACK.

Companies are focused on gathering data to sell. They are NOT focused on your security and safety.

Introducing “the internet of things.” (IOT) If it’s connected to the internet, it can be accessed and hacked.

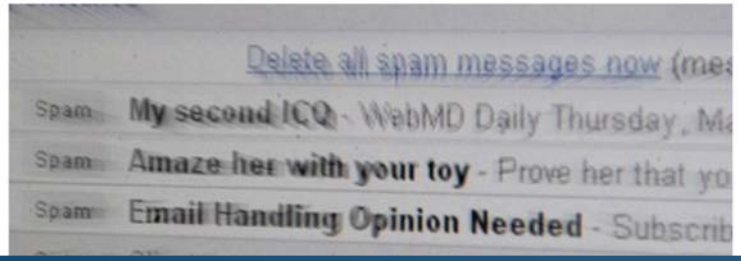
BBC Sign in | Home | News | Sport | Reel | Worklife | Travel

Home | War in Ukraine | Coronavirus | Climate | Video | World | US & Canada | UK | Business | Tech | Science

Tech

Fridge sends spam emails as attack hits smart gadgets

17 January 2014



MIKE CLARKE

The fridge was one of 100,000 devices used as part of the spam attack

A fridge has been discovered sending out spam after a web attack managed to compromise smart gadgets.

The fridge was one of more than 100,000 devices used to take part in the spam campaign.

Uncovered by security firm Proofpoint the attack compromised computers, home routers, media PCs and smart TV sets.

The attack is believed to be one of the first to exploit the lax security on devices that are part of the "internet of things".

Poor protection

The spam attack took place between 23 December 2013 and 6 January this year, **said Proofpoint in a statement**. In total, it said, about 750,000 messages were sent as part of the junk mail campaign. The emails were routed through the compromised gadgets.

About 25% of the messages seen by Proofpoint researchers did not pass through laptops, desktops or smartphones, it said.

Instead, the malware managed to get itself installed on other smart devices such as kitchen appliances, the home media systems on which people store copied DVDs and web-connected televisions.

Many of these gadgets have computer processors onboard and act as a self-contained web server to handle communication and other sophisticated functions.

INNOVATION

My Toaster Hacked The Pentagon: What You Can Do To Secure Your IoT Devices

Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

POST WRITTEN BY

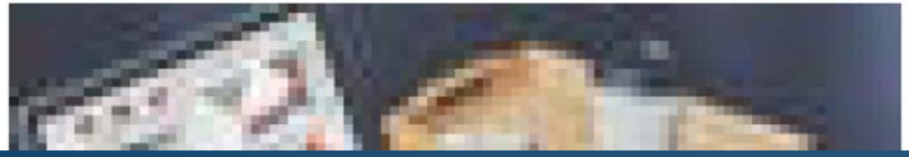
Forbes Technology Council

Successful CIOs, CTOs & executives from Forbes Technology Council offer firsthand insights on tech & business.

Mar 3, 2017, 07:00am EST

As more devices join the internet of things, from toasters and washers to refrigerators and home thermostats, the number of avenues for attacks by ill-meaning hackers widens. This can leave end users with the mess of stolen passwords, damaged homes or lost privacy.

Despite these risks, networking devices can add value to owner's lives. However, security steps need to be taken to prevent trouble, and consumers cannot assume that the company they purchased an appliance from has updated every device they've sold. Aware of the dangers, Forbes Technology Council experts offer these methods for end users to use to help protect their devices from being hacked.



Home › Tech › LG's Smart Fridge Is Giving Customers A Guilt Trip

LG's Smart Fridge Is Giving Customers A Guilt Trip

Smart home appliances can often prove to be equally as annoying as they are useful, as one LG smart fridge owner recently found out and explained.

BY JOSEPH SCOTTING
PUBLISHED SEP 10, 2021

LG smart fridges can guilt-trip their owners for opening the door too often, according to one Twitter user. LG was one of the original pioneers of smart appliances, with the company's first internet fridge unveiled in 2000. Since then, smart appliances have exploded in popularity, thanks to their ability to remotely tell owners the temperature of their food, when ice is ready, and when their laundry is finished. While a convenient addition to one's daily life, many owners probably wouldn't expect their fridge to routinely email them.

Introducing “the internet of things.” (IOT) If it’s connected to the internet, it can be accessed and hacked.

Ring hacked: doorbell and camera security issues

Imagine your kids playing with the dog when suddenly a voice starts speaking to them from your pet camera. Or a stranger walks into your house instead of the friend you just saw in your doorbell camera. These are real stories that happened to ordinary people, thanks to hacked Ring devices. Read on to learn more about them.

Paulius Ilevičius

Dec 23, 2021

5 min read

Introducing “the internet of things.” (IOT) If it’s connected to the internet, it can be accessed and hacked.

Introducing “the internet of things.” (IOT) If it’s connected to the internet, it can be accessed and hacked.

Introducing “the internet of things.” (IOT) If it’s connected to the internet, it can be accessed and hacked.

THE DEVICES TALK TO ONE ANOTHER.

Internet of things devices use APIs, devices such as:

Garmin Health API, Google Assistant, Withings, Apple Homekit, Alazon Alexa, Udibots, and many, many (many) more.

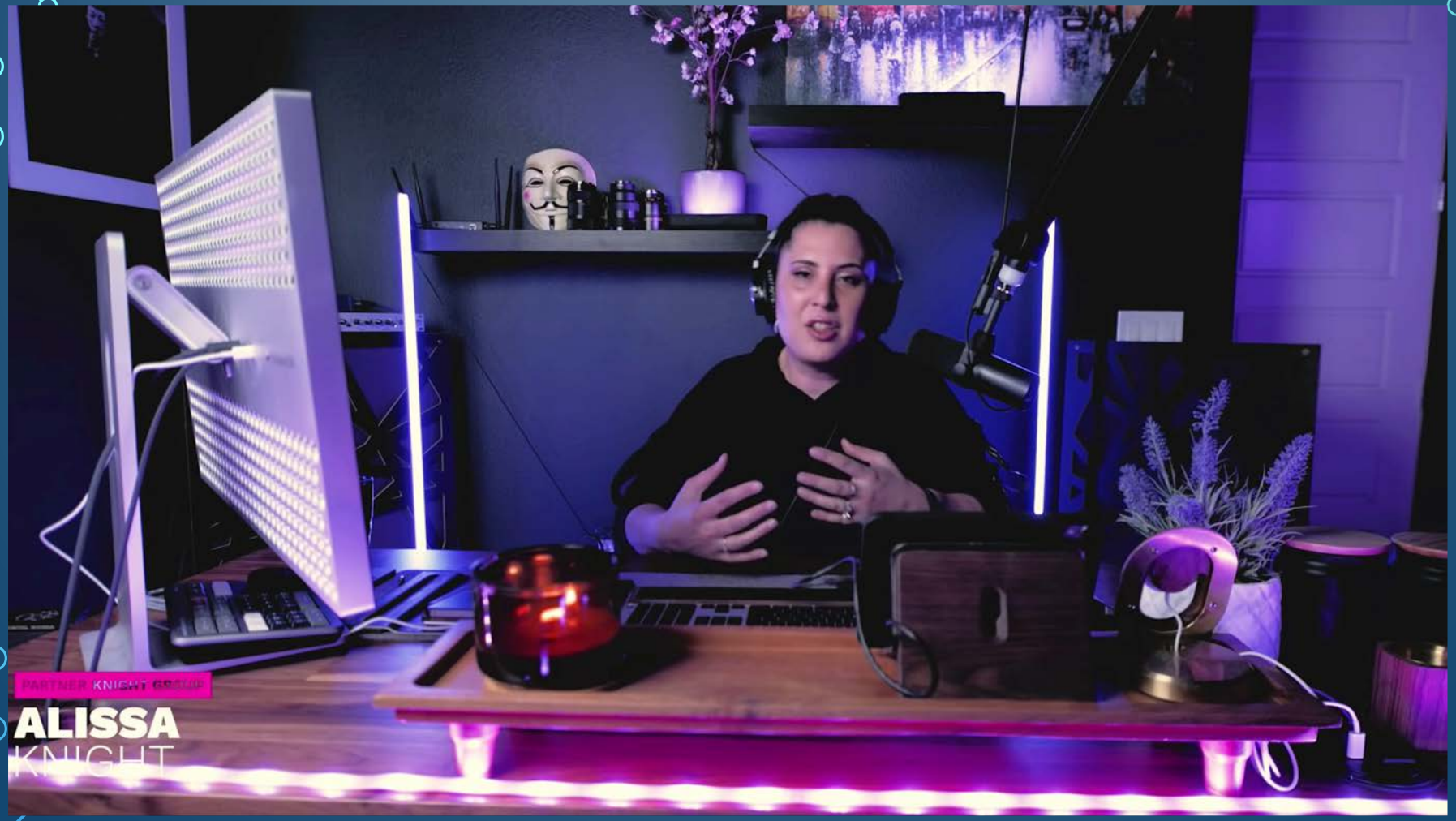
Think of: Wearables, exercise, sleep trackers collecting data on steps, sleep, calories, heart rate, stress, intensity minutes, body composition voice control over phone applications, speakers, smart displays, automobiles, watches, laptops, TV, Nest, measuring devices, such as scales and blood pressure monitors, that can send health information directly to the internet.

Apple Homekit: lights, thermostats, garage doors, etc. could all be controlled by voice. Apple HomeKit API is accessible via the Apple iOS8 SDK.

Amazon Alexa: controls TVs, alarms, door locks, lights, and any number of other smart home devices.

Ubidots: This platform (like many others) can send data to the cloud from any Internet-enabled device.

Alissa Knight, expert on API Hacking, employed by law enforcement to protect law enforcement vehicles' APIs.



Introducing "the internet of things." (IOT) If it's connected to the internet, it can be accessed and hacked.

THESE HACKERS WERE NOT LOOKING FOR FINANCIAL DATA…

What if they listened for PASSWORDS, personal financial information?

Have you ever had a confidential conversation with a client on the phone while standing in your kitchen?

Do you have a smart toaster?

Do you have a ring device?

What about an "Alexa" device?

Apple T.V.?

"Hey Siri, don't listen to the private conversation I'm having with my client."

WHY DO WE CARE IF OUR "SMART TOASTER" LISTENS TO US?

Is the "smart toaster" listening to our conversations and sensitive information? Can hackers infiltrate the devices?

What about Alexa?

Hey "Alexa!" don't violate attorney-client privilege.

IS MY PHONE LISTENING TO ME?

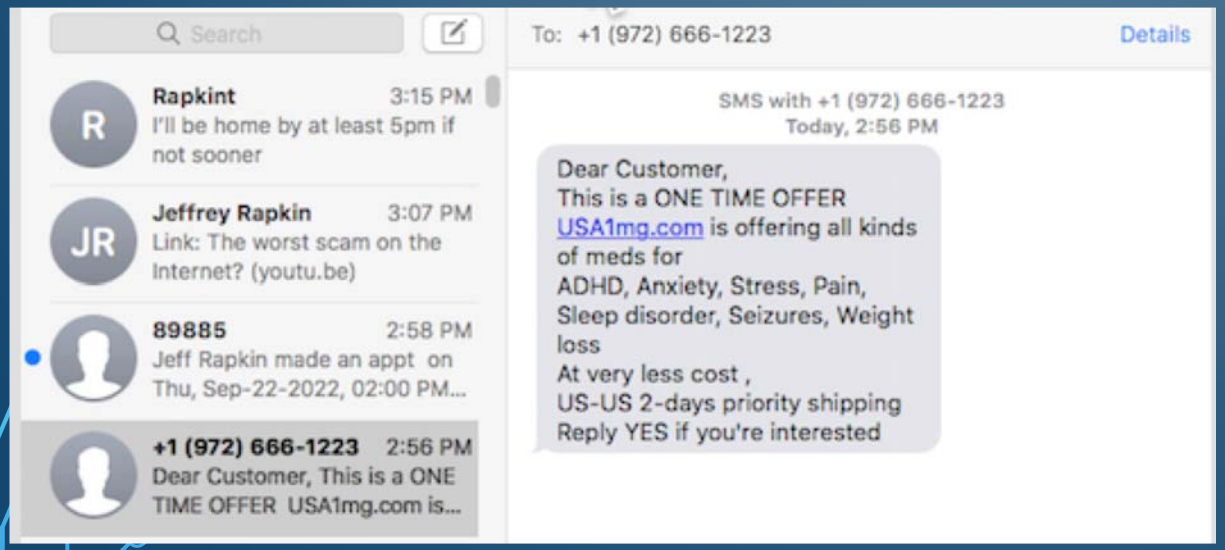
Social Engineering…

IS MY PHONE LISTENING TO ME?

Social Engineering…

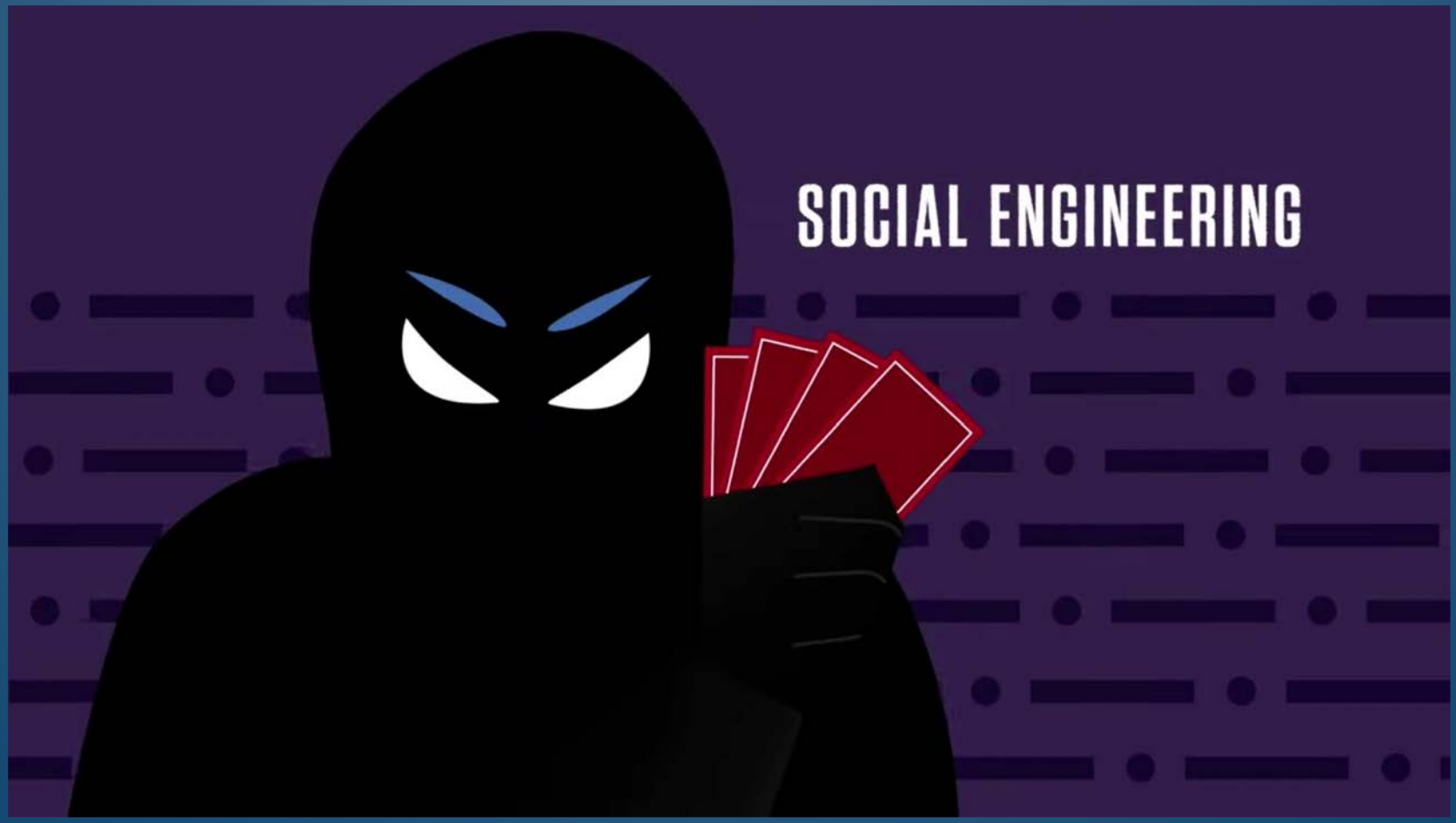
WHAT IS "SOCIAL ENGINEERING?"

"Social Engineering" is a term used to describe specific activity of cybercriminals (or advertisers) when they design attacks (or ads) for a specific person or group. The attack is designed to appeal to the target by using the target's interests, behaviors, motivations, wants, and needs. Social engineering is based on manipulation.

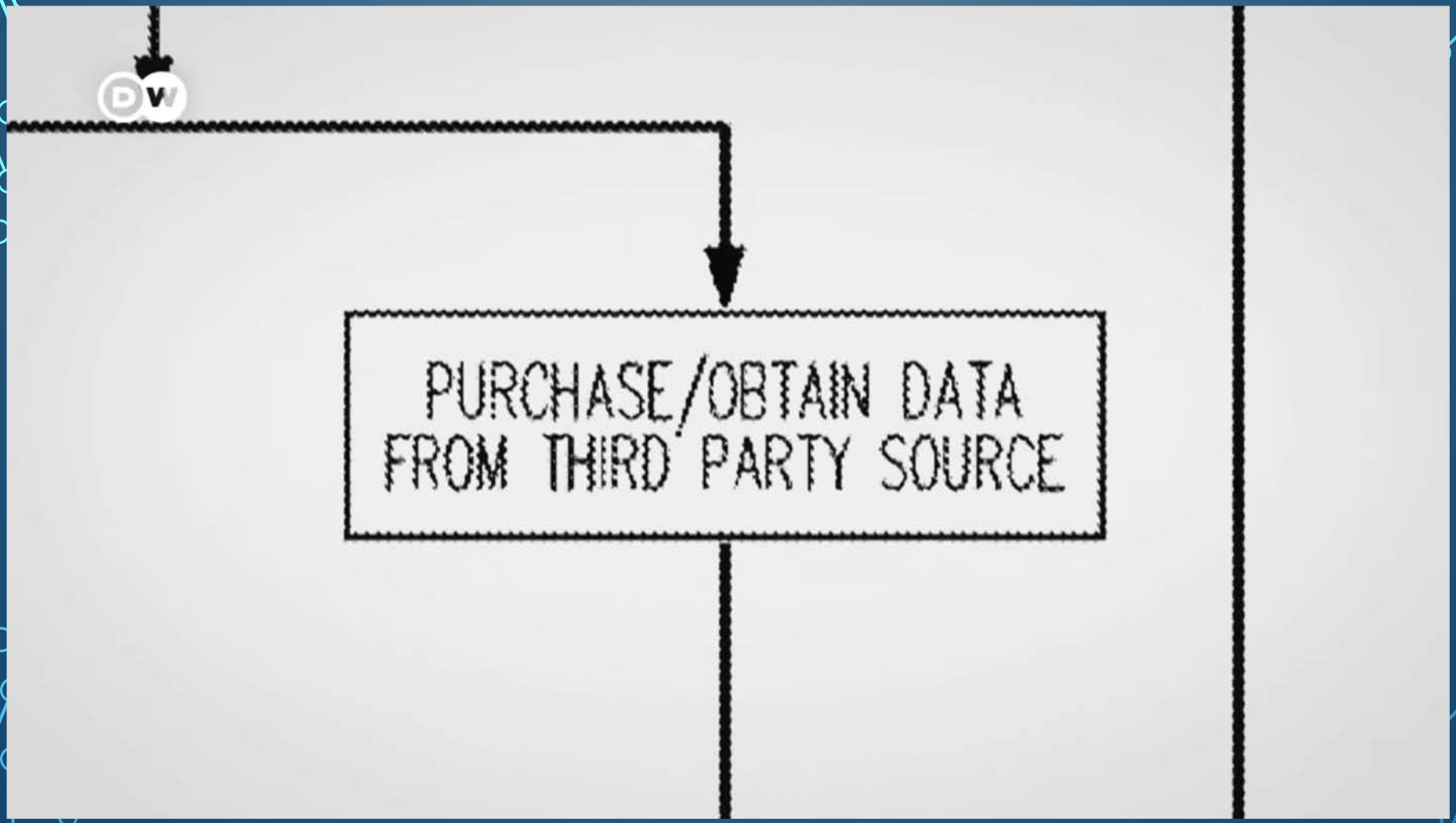


This is Social Engineering directed at me.
I received it 07/28/2022.
Any ideas why I might have gotten this?
(This is "Smishing" by the way.)

SOCIAL ENGINEERING



Social Engineering…



Social Engineering…

I HATE COOKIES. (THE INTERNET KIND, I MEAN.)

HTTP cookies, or internet cookies, are built specifically for Internet web browsers to track, personalize, and save information about each user's session. Internet Cookies are used for:
Session management. For example, cookies let websites recognize users and recall their individual login information and preferences, such as sports news versus politics. **Personalization.** Customized advertising is the main way cookies are used to personalize your sessions. You may view certain items or parts of a site, and cookies use this data to help build targeted ads that you might enjoy. **Tracking.** Shopping sites use cookies to track items users previously viewed, allowing the sites to suggest other goods they might like and keep items in shopping carts while they continue shopping.

Cookies were invented in 1994 by "Netscape." (Remember "Netscape" before it was (brutally) murdered by Microsoft? (Bill Gates)

They were used primarily to load websites faster and prevent servers from having to store your computer's info. We don't need these anymore. They are still used today, but for (what I call) nefarious purposes, such as tracking. (That's why the EU made it a law that they have to tell you about them now.)

DISABLE COOKIES?

Turn cookies on or off

To use your Google Account on a browser (like Chrome or Safari), turn on cookies if you haven't already.

Important: If you get a message that cookies are turned off, you need to turn them on to use your account.

Computer | Android | iPhone & iPad

In Chrome

1. On your computer, open Chrome.
2. At the top right, click More ⋮ > **Settings**.
3. Under "Privacy and security," click **Site settings**.
4. Click **Cookies**.
5. From here, you can:
   - Turn on cookies: Next to "Blocked," turn on the switch.
   - Turn off cookies: Turn off **Allow sites to save and read cookie data**.

SNOWDEN EXPLAINS TRACKING

Edward Snowden is not the ”wikileaks guy.” (That was Julian Assange.) Snowden (in 2013) blew the whistle on USA’s surveillance (often illegal) tactics.

BTW, He’s still in hiding. Being tracked is a big issue for him.)

IS GOOGLE LOCATION TRACKING GOOD OR BAD?

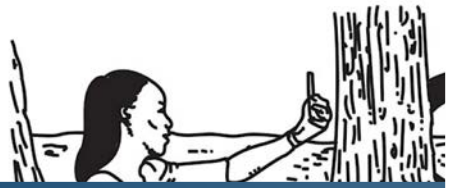
engadget Sections Login

B@d P@sswOrd Examining infosec and our ever-eroding privacy. See all articles

How Google's location-tracking issue affects you

Watching Google watch us.

V. Blue
@violetblue
August 17, 2018
3:15 PM

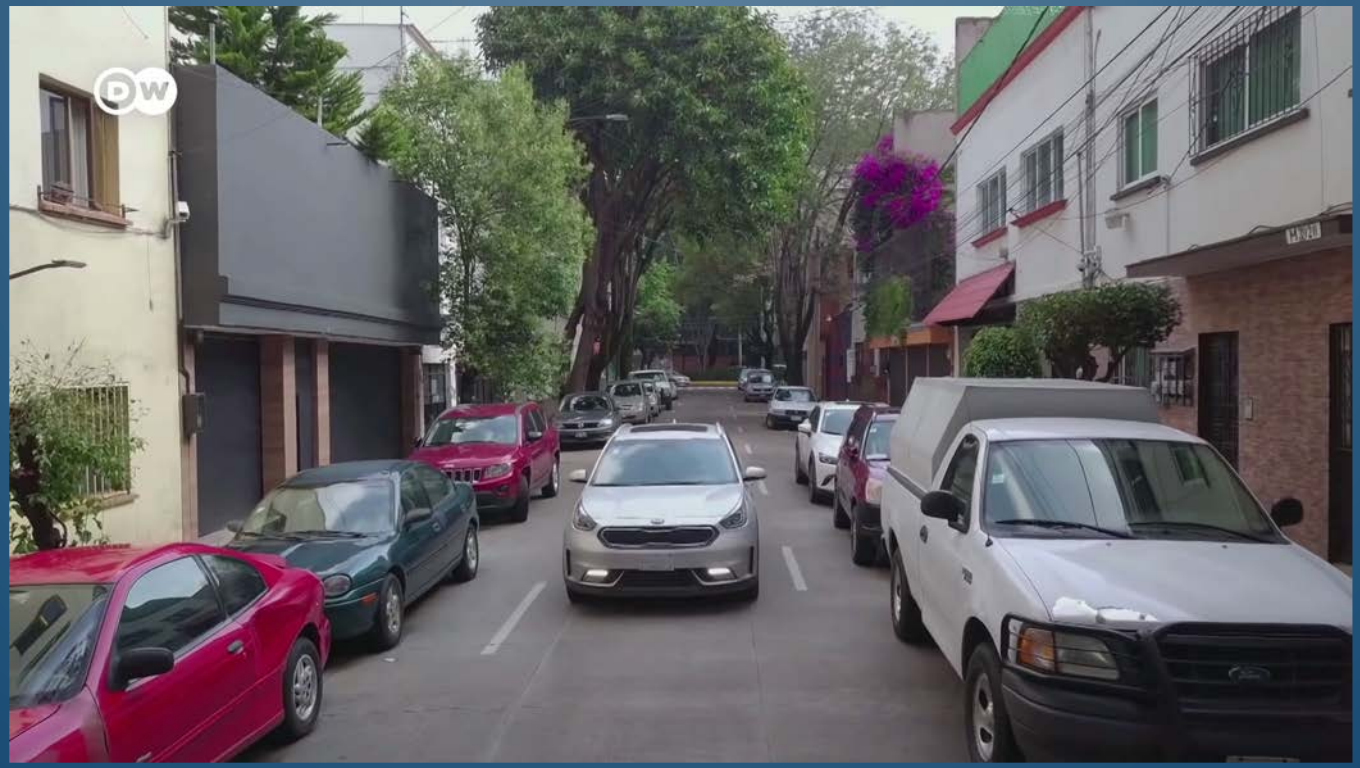


This week, the Associated Press published the findings of its investigation showing that Google tracks your locations even if you've shut off the Location History setting -- which is what the company says to do if you don't want Google tracking you. Google's Manage or delete your Location History page states, "You can turn off Location History at any time. With Location History off, the places you go are no longer stored."

"That isn't true," writes the AP. "Even with Location History paused, some Google apps automatically store time-stamped location data without asking.

Check my location history?

HAS ANYONE EVER HEARD OF PEGUSAS?



WE ARE BEING LISTENED TO. WE ARE BEING TRACKED…

WE ARE ALSO BEING HACKED.
HOW DOES ”HACKING” ACTUALLY WORK?

Most people will never be victims of a “brute force” attack. We would be the victims of social engineering. The attacks would be specifically directed at us.

This is hacking the ”person,” not necessarily the device and methods of attack include (but are not limited to) email redirects, phishing, thumbdrives with keyloggers, password hacking, and any other method to “trick” you into opening the door.

BE AWARE!

Phishing

Pharming

Smishing

Social Media Messenger Scams

Romance/online dating scams

Emergency (Grandparent) Scams

Online Marketplace Scams

“Free” Gift Offers

Malware

Advance Fee Scams

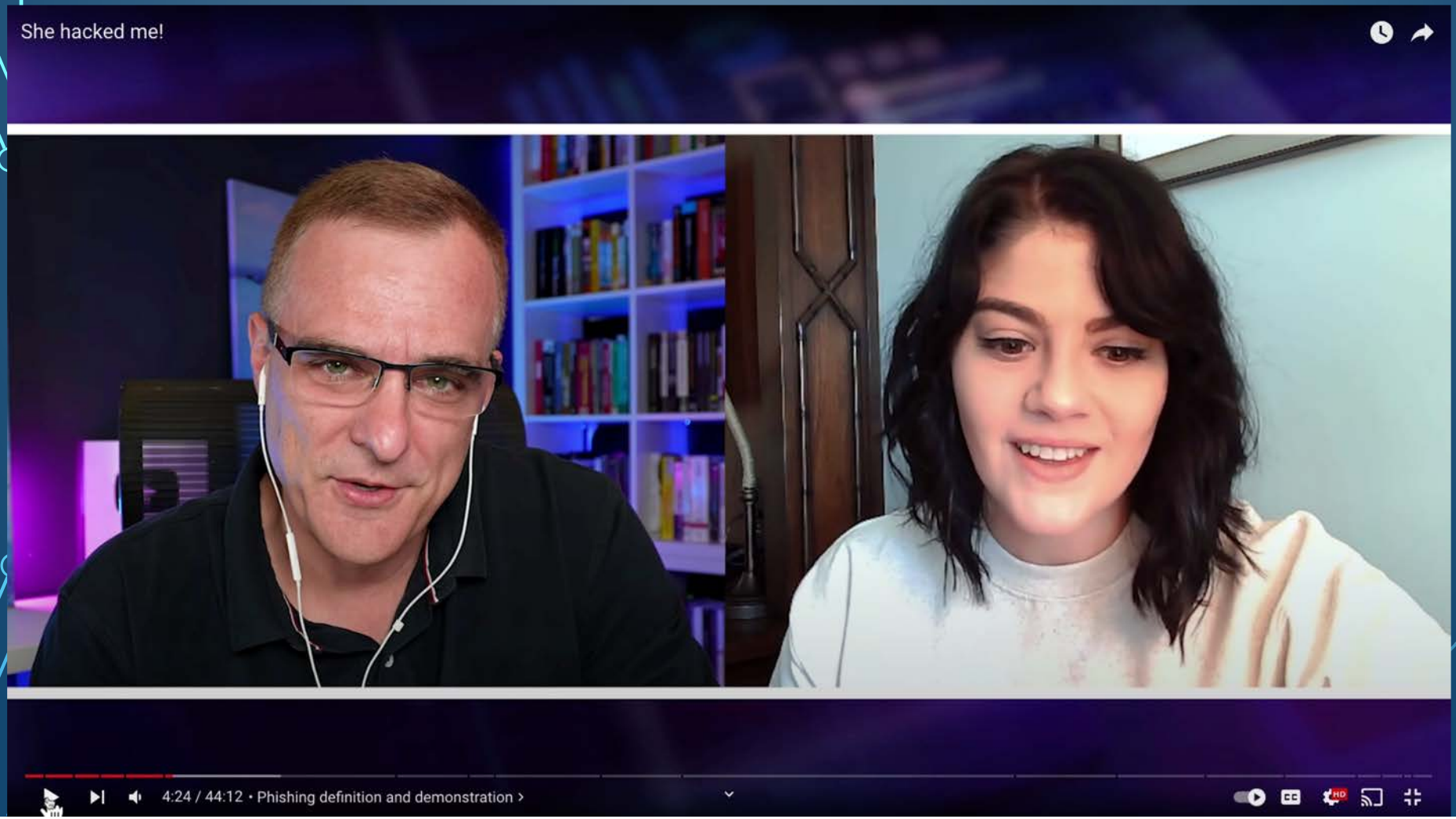
Foreign Money (Nigerian Prince)

Spoofing

WHAT IS "PHISHING?"

The criminal poses as a trusted, legal, legitimate, source in order to fool you into providing sensitive data, criminal then uses the information to steal from you (obviously) or commit identity theft. Malware is usually left behind for further attacks.

WHAT IS “PHISHING?”



WHAT IS “PHISHING?” (YES, AMAZON WILL HOST YOUR ILLEGAL ACTIVITIES FOR FREE.)

WHAT IS “PHARMING?”

Pharming uses ”DNS Poisoning” or ”Spoofing” to redirect your device to a fraudulent website designed to capture sensitive information.

PHISHING AND PHARMING ARE SIMILAR, BUT HAVE SOME KEY DIFFERENCES IN HOW THEY WORK.

PHISHING

* Criminal tricks victim into providing sensitive information through email or text message

* Involves a fraudulent link to a website which then attempts to gain the user's information

* Is an attack directed at one person at a time

* Phishing attacks are relatively easy to initiate as well as identify

* Requires unsuspecting victim to click on malicious code in their inbox

PHARMING

* Seeks sensitive data through domain spoofing

* Works by exploiting DNS system and is harder to identify than Phishing

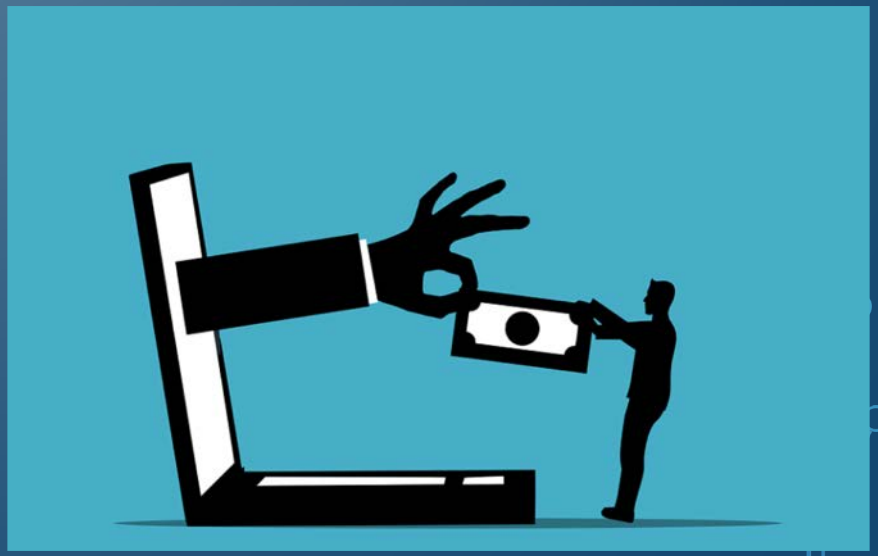
* Targets multiple victims at a time by using a technique called "DNS Poisoning." Works by infusing false info into DNS, redirecting users to illegitimate websites designed to steal data.

* Spyware removal tools are useless because technically, there is no malware on the end-users' computers.

ATTORNEYS WHO HAVE BEEN SCAMMED

Some Examples Include:

- Scammers pretending to be from Bar Association
- Legal Representation Scams
- Debt Recovery Assistance Scams
- Family Law Attorney Scam
- ”Advance Fee Fraud”



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

June 30, 2022

Alert Number
I-063022-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Attorney Trust Account Scam Promises High-Dollar Commissions on Medical Equipment Purchases

The FBI Minneapolis Field Office, in coordination with the Internet Crime Complaint Center and the Office of Private Sector (OPS), warn of an attorney trust account scam involving acquisition of medical equipment. The scam has resulted in approximately $2 million in losses to date.

Method used by the criminal actors in the attorney trust account scam:

- A criminal actor posing as a would-be client contacts an attorney either listed on a professional networking site or claiming to have found their information on such sites, requesting their services in reviewing a lease, loan, or purchase agreement for medical equipment. The attorney is also requested to serve as an escrow agent for the client.
- An individual posing as a broker representing a client emails the attorney an offer letter, and sends a cashier's check by mail.
- The cashier's check for settlement is received, and deposited into the attorneys (or firm's) trust account.
- The client then requests the attorney wire transfer a portion of the funds from the trust account to another account, most often located in Mexico.
- After the funds are wired as directed (some attorneys doing so before the cashier check has cleared), the attorney learns the check was fraudulent, and is liable to the bank for the funds, if not recovered.

The scam is successful for several assumed reasons:

- The perpetrators entice lawyers with potential high dollar commissions on transactions involving multi-million dollar medical equipment such as MRI machines, ventilators, and CT scanners.
- A potential need for new clients or quick cash flow by the attorney, may lead the attorney to take short-cuts when verifying information, following firm policies, or waiting for funds to clear.
- The criminal actors place pressure on the attorney to act quickly in sending wires and refer to the importance of the business transaction or short time frames.
- The criminal actors use cashier's checks not easily detectable for fraud, provide websites that appear legitimate, and sometimes pose as legitimate medical companies.

To reduce the chances of becoming a victim, verify the validity of any payment method and wait for funds to clear, especially checks, before depositing or utilizing the funds.

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

June 10, 2019

Alert Number
I-061019-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Cyber Actors Exploit 'Secure' Websites In Phishing Campaigns

Websites with addresses that start with "https" are supposed to provide privacy and security to visitors. After all, the "s" stands for "secure" in HTTPS: Hypertext Transfer Protocol Secure. In fact, cyber security training has focused on encouraging people to look for the lock icon that appears in the web browser address bar on these secure sites. The presence of "https" and the lock icon are supposed to indicate the web traffic is encrypted and that visitors can share data safely. Unfortunately, cyber criminals are banking on the public's trust of "https" and the lock icon. They are more frequently incorporating website certificates—third-party verification that a site is secure—when they send potential victims emails that imitate trustworthy companies or email contacts. These phishing schemes are used to acquire sensitive logins or other information by luring them to a malicious website that looks secure.

RECOMMENDATIONS:

The following steps can help reduce the likelihood of falling victim to HTTPS phishing:

- Do not simply trust the name on an email: question the intent of the email content.
- If you receive a suspicious email with a link from a known contact, confirm the email is legitimate by calling or emailing the contact; do not reply directly to a suspicious email.
- Check for misspellings or wrong domains within a link (e.g., if an address that should end in ".gov" ends in ".com" instead).
- Do not trust a website just because it has a lock icon or "https" in the browser address bar.

June 17, 2020

PRACTICE POINTS

Lawyer Beware: Four Tips to Avoid Email Scams Targeting Lawyers

Advance-fee fraud does not always come fro
it always target internet newbies. Learn how
growing trend of nefarious "clients."

By Paula M. Bagger

Share:

A prospective client contacts you seeking represer
but he emails you background documents on the
signs your engagement letter.

Almost immediately, the matter settles. The adverse party sends a large check, made out to you for the benefit of your client. You notify your client and deposit the check in your attorney trust account. Your client tells you that he needs the funds immediately and provides his wire information.

What do you do?

These are the facts of several currently circulating email scams targeting lawyers. There are several variations: One involves a claim for unpaid severance from an Ohio health care company; another involves the collection of overdue loan payments from a Massachusetts restaurant company. The purported adverse party is often a real company and the underlying documents put together with a sophisticated touch—there are no "Nigerian princes" involved. But the check is counterfeit and the goal of the scam is to cause the attorney to disburse funds before learning that the check is no good.

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Sep 18, 2018

Alert Number
I-091818-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Cybercriminals Utilize Social Engineering Techniques To Obtain Employee Credentials To Conduct Payroll Diversion

The IC3 has received complaints reporting cybercriminals are targeting the online payroll accounts of employees in a variety of industries. Institutions most affected are education, healthcare, and commercial airway transportation.

METHODOLOGIES

Cybercriminals target employees through phishing emails designed to capture an employee's login credentials. Once the cybercriminal has obtained an employee's credentials, the credentials are used to access the employee's payroll account in order to change their bank account information. Rules are added by the cybercriminal to the employee's account preventing the employee from receiving alerts regarding direct deposit changes. Direct deposits are then changed and redirected to an account controlled by the cybercriminal, which is often a prepaid card.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

March 20, 2020

Alert Number
I-032020-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic

Phishing Emails. Look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government. While talk of economic stimulus checks has been in the news cycle, government agencies are *not* sending unsolicited emails seeking your private information in order to send you money. Phishing emails may also claim to be related to:

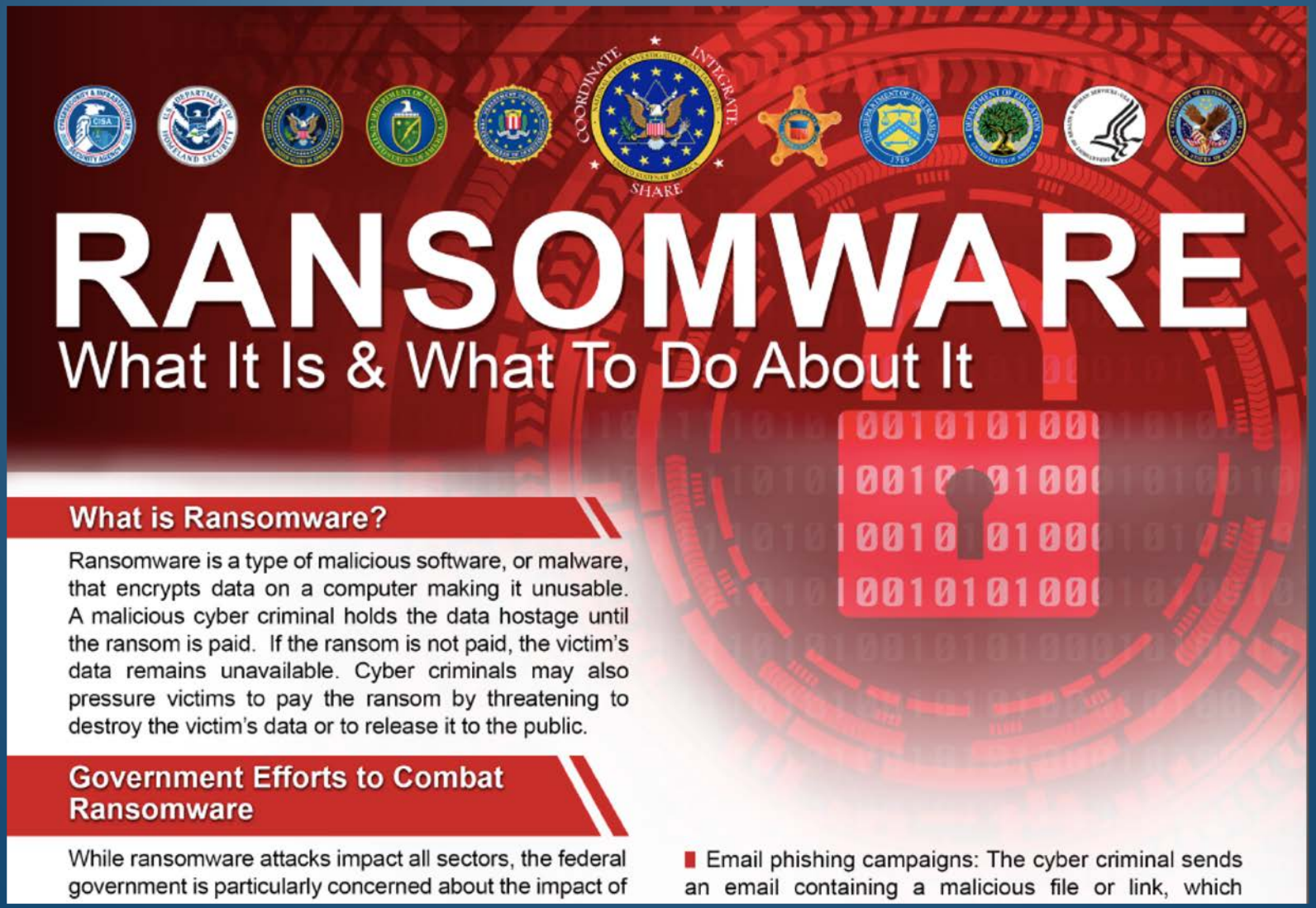
- Charitable contributions
- General financial relief
- Airline carrier refunds
- Fake cures and vaccines
- Fake testing kits

Counterfeit Treatments or Equipment. Be cautious of anyone selling products that claim to prevent, treat, diagnose, or cure COVID-19. Be alert to counterfeit products such as sanitizing products and Personal Protective Equipment (PPE), including N95 respirator masks, goggles, full face shields, protective gowns, and gloves. More information on unapproved or counterfeit PPE can be found at www.cdc.gov/niosh. You can also find information on the U.S. Food and Drug Administration website, www.fda.gov, and the Environmental Protection Agency website, www.epa.gov. Report counterfeit products at www.ic3.gov and to the National Intellectual Property Rights Coordination Center at iprcenter.gov.

FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic

Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them. Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits. The FBI advises you to be on the lookout for the following:

Fake CDC Emails. Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received.


RANSOMWARE
What It Is & What To Do About It
What is Ransomware?
Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.
Government Efforts to Combat Ransomware
While ransomware attacks impact all sectors, the federal government is particularly concerned about the impact of
Email phishing campaigns: The cyber criminal sends an email containing a malicious file or link, which

WHAT IS RANSOMWARE?

Index

Cyber insurance is as dynamic as the companies it protects and is consequently far from standardized. However, some of the issues that cyber liability insurance typically covers include:

- Data loss, recovery, and recreation
- Business interruption/ loss of revenue due to a breach
- Loss of transferred funds
- Computer fraud
- Cyber extortion

Important Note: Errors and omissions insurance is not cyber insurance and cannot serve as a substitute for proper cyber insurance, even if the E&O policy has a technology error rider.

If hackers expose or steal personal information, such as Social Security numbers, driver's' license number (in some states), address, and bank account information, a cyber liability insurance policy pays for:

- **Notification Costs:** This expense is significant because the company bears the burden of both identifying potential victims, which requires an

CONCLUSION

Backup. (You must!) And maintain them!
Unless you know it, don't click (or tap) on it.
Limit what is listening to you, at least in your office.
Go into preferences and take control of trackers, cookies, and other vulnerabilities.
Use strong passwrds and change them on a regular basis.
Use two-factor authentication.
Always update. (they are almost always about security)
Check domain names and certificates before putting in login info.
If suspicious, switch browsers and type in the url yourself.
Don't click in links in emails.
Keep firewalls on. (And consider a reputable VPN)
Https:// is better than Http://
Limit the personal information you give out (avoid being "socially engineered!")
You will not be contacted by a bank or legitimate site which then asks for your login or other personal info.
Avoid getting hooked by pressure tactics. If suspicious, slow down, ask for help.
If you get attacked, turn everything off, pull the plugs and get help.