Securing Law Practice Technology and Reporting CLE

Host: WV State Bar
CLE: 3 credits in Law Office Management
Time: 1:00 p.m. to 4:00 p.m. EST

Speakers/Topics:
Danielle Cox, WV Office of Technology
"Cybersecurity Essentials – Making yourself less of a target"
Todd Sexton, Identillect
"Is Your Mobile Device at Risk"
Angela Volk and Michael Mellace, WV State Bar
"Reporting CLEs and Using State Bar Technology"

The webinar will focus on technology issues including how to keep your firm/office cyber secure, encrypting email, and how to report CLE. You and your employees are encouraged to attend the live webinar. Because Zoom capacity is limited, the Bar requests that attendees participate as a social-distance group rather than individually.

Todd Sexton, Chief Executive Officer, Identillect Technologies

Todd Sexton is an accomplished speaker and author in the field of cyber-security and data handling regulation. Over the past 15 years, Todd has focused on cyber-security compliance in an ever-changing landscape of regulatory requirements. Specifically focused on helping lawyers understand technology, he spends a tremendous amount of effort assisting the legal community on the advancing data-handling regulations, cybersecurity threats, and wire fraud/data tampering.

Is your mobile device at risk?

Todd Sexton, MBA
CEO, Identillect Technologies
Cyber-Security Expert

WHAT YOU ARE GOING TO LEARN...

01

02

03

04

DATA LEAKAGE
Loss of business information by inadvertent decisions on where information is kept.

SOCIAL ENGINEERING
Utilizing trickery to gain access to information, account access, or network access.

Wi-Fi INTERFERENCE
A mobile device is only as secure as the network through which it transmits data.

OUT-OF-DATE DEVICES
Outdated software on mobile devices tends to be ineffective on mandating and pushing updates

MORE OF WHAT YOU WILL LEARN...

05

06

07

08

CRYPTOJACKING ATTACKS

A criminal uses a device to mine for cryptocurrency without the owner's knowledge.

POOR PASSWORD HYGIENE

Reused passwords and lack of 2FA is greatly concerning

PHYSICAL DEVICE BREACHES

Greater than 35% of businesses do not mandate appropriate encryption protocols

MOBILE AD FRAUD

Fraud created by imposter ads

Cyber Threats Impact on Rules & Opinions

- A lawyer shall make Reasonable Efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

- Define Reasonable: At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology to protect client communication"

- Reasonable for Technology: lawyers must exercise reasonable efforts when using technology in communicating about client matters.
-
- Risk Assessment and Effectively: "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify they are effectively implemented, and ensure that they are continually updated in response to new developments.

Data Leakage

- Firms have a nearly 28% chance of experiencing at least one incident in the next two years
- This is triggered by users inadvertently making ill-advised decisions about which apps can see and transfer their information.
- Remember this every time you install a new app and it requests access to specific information .
- Suggest MDM software or mobile device management

Mobile Device Management

Mobile Device Management Software (MDM)

A form of security application that enables an IT department to manage, monitor, and secure employees' mobile devices

Google MDM

Manage your organization's mobile devices. If you have the legacy free edition of G Suite, upgrade to G Suite Basic to get this feature. You can use Google Mobile Management to manage, secure, and monitor mobile devices in your organization.

Microsoft MDM

The built-in Mobile Device Management (MDM) for Office 365 helps you secure and manage your users' mobile devices. You can create and manage device security policies, remotely wipe a device, and view detailed device reports.

Email Security

Encryption is a mathematical formula to prevent unauthorized access

- Secure all client communication
- Control communication
- Restrict printing, forwarding, and unauthorized access
- Email retraction
- Enforce organization security protocols
- Allow for inbound security
- Large file secure transfer

Security Standards

- End-to-End Encryption
- AES 256 as a Standard
- Select a product which focuses on lawyers
- Make sure it plugs into your existing email system

Delivery Trust® Unique Offering for Bar Members

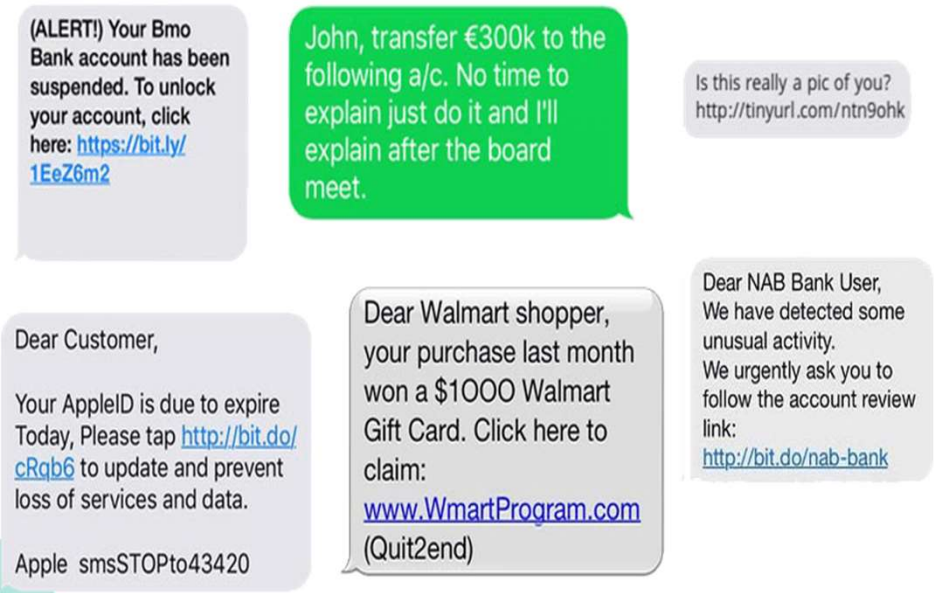
Secure your email simply and inexpensively

- Benefits:
  - Secure all client communication
  - Control communication
    - Restrict printing, forwarding, and unauthorized access
    - Email retraction
    - Enforce organization security protocols
  - Allow for inbound security
  - Large file secure transfer

Social Engineering

- A staggering 91% of cybercrime starts with email, according to a 2018 report by security firm FireEye.
- Rely on tactics like impersonation to trick people into clicking dangerous links or providing sensitive info.
- Mobile email clients display only a sender's name — making it especially easy to spoof messages and trick a person into thinking an email is from someone they know or trust.
- 83% of phishing attacks over the past year took place outside the inbox — in text messages or in apps like Facebook Messenger and WhatsApp along with a variety of games and social media services.
- Solution – Utilizing 2FA
- Or utilize physical security keys like Google's Titan or Yubico's YubiKeys or via Google's on-device security key option

Smishing Attack



- Smishing: is a form of social engineering that exploits SMS, or text, messages.
- Can contain links to such things as web pages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number.
- Increases the likelihood that users will fall victim to engineered malicious activity.

Public Wi-Fi Interference

Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can use your connection. The typical indoor broadcast range of an access point is 150–300 feet. Outdoors, this range may extend as far as 1,000 feet. These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files.

Evil Twin Attacks

An adversary gathers information about a public network access point, then sets up their system to impersonate it. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet.

Wireless Sniffing

Many public access points are not secured and the traffic they carry is not encrypted. Because your connection is being transmitted "in the clear," malicious actors could use sniffing tools to obtain sensitive information such as passwords or credit card numbers

Wi-Fi

WEP

Inadequate security for home or office

WPA

Inadequate security for home or office

WPA2

Adequate security for home or office

WPA3

Adequate security for home or office

Did you know?

Only use sites that begin with “https://” when online shopping or banking

Using your mobile network connection is generally more secure than using a public wireless network.

VPN (Virtual Private Network)

What is a VPN?

- This is a service which lets you access the web safely and privately by routing your connection through a server and encrypting online actions.

Is a VPN Legal to use?

- Yes, in North America and Western Europe … Some countries outlaw them like China

Does a VPN make you completely invisible?

- No

What do most VPN logging policies log?

- User activity
- IP Address
- Devised Used
- Payment Logs
- Connectivity/ disconnection timestamps

Out-of-Date Device

- Most manufacturers are embarrassingly ineffective at keeping their products up to date — both with operating system (OS) updates and with the smaller monthly security (Especially Android)
- Google is working on an all-in-one android update anticipated to be out by summer 2021.

Update Software

Software's to keep updated

- Operating System Update
- Browser Software Update
- Software Suite Update (Microsoft, Apple, etc.)
- VPN Update
- Wi-Fi Software Update
- Firewall Software Update
- Mobile Device Update

Cryptojacking Attacks

- Cryptojacking is a type of attack where someone uses a device to mine for cryptocurrency without the owner's knowledge
- Experience slow processor speed, low battery life, and components overheating --- there was a huge surge from 2017-2019
- Google play store and iOS App Store has banned crypto mining apps this threat has decreased but still can be an issue when using open streaming applications

Poor Password Hygiene

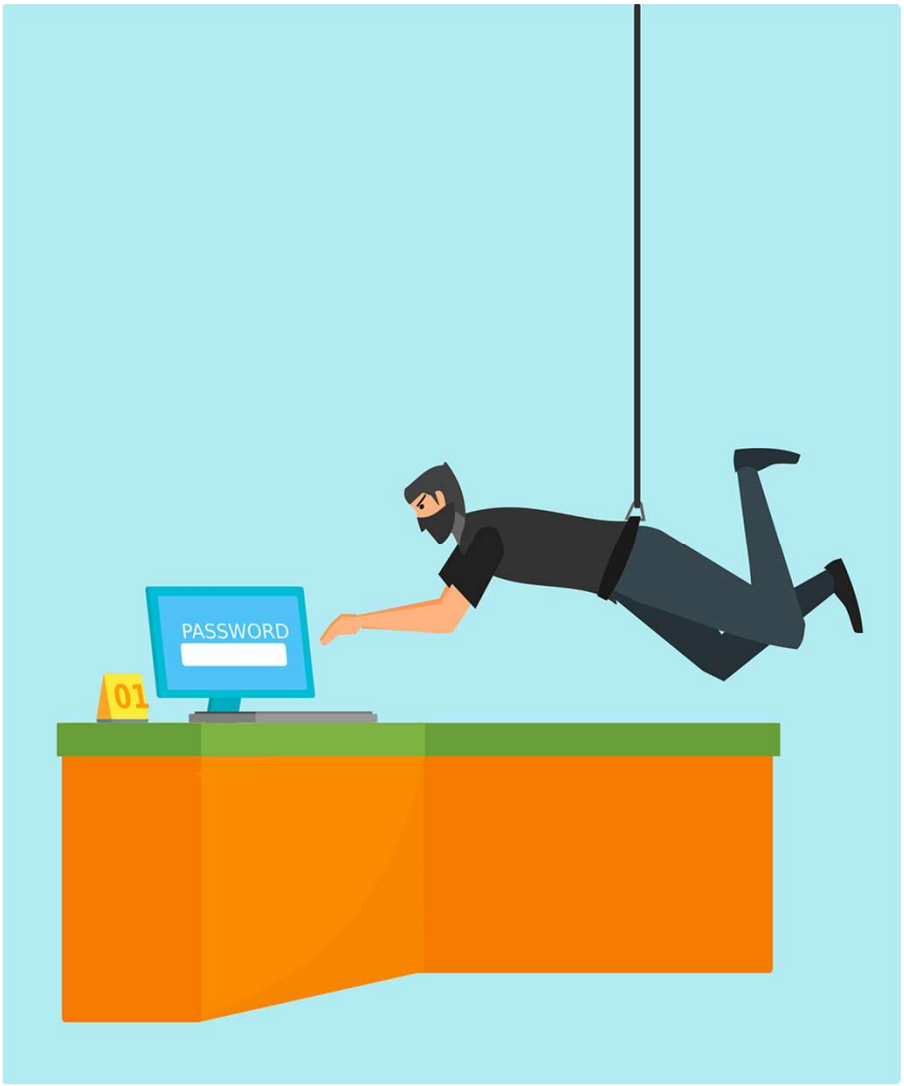
- Google's recent survey determined over 50% of Americans
  - ✔ Reuse passwords over multiple accounts
  - ✔ Many are not using 2FA
  - ✔ Even less use a password manager
  - ✔ Examples: 1Password, Bitwarden, Dashlane, KeePass, Keeper Security, LastPass

- What constitutes a strong password?
  - ✔ These passwords should be at least 12 characters long… longer is better
  - ✔ Good passwords can't contain memorable keyboard paths
  - ✔ Password strength isn't personal
  - ✔ A good password should be unique
  - ✔ Use Symbols, numbers, and Capitalization
  - ✔ Examples of a good passwords (X5j13$#eCM1cG@Kdc)

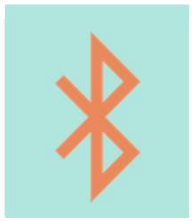
- **CONSIDER PASSWORD GENERATOR and PASSWORD KEEPER**

Physical Device Breach

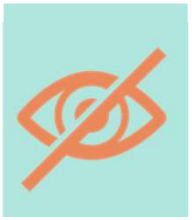
- 35% of professionals indicated their work devices had no mandated measures in place to secure accessible corporate data.
- Ensure you have a corporate policy requiring corporate standards are enforced (MDM)
- Bluetooth Visibility
- Charging with Computer



Bluetooth



Turn it off when not in use



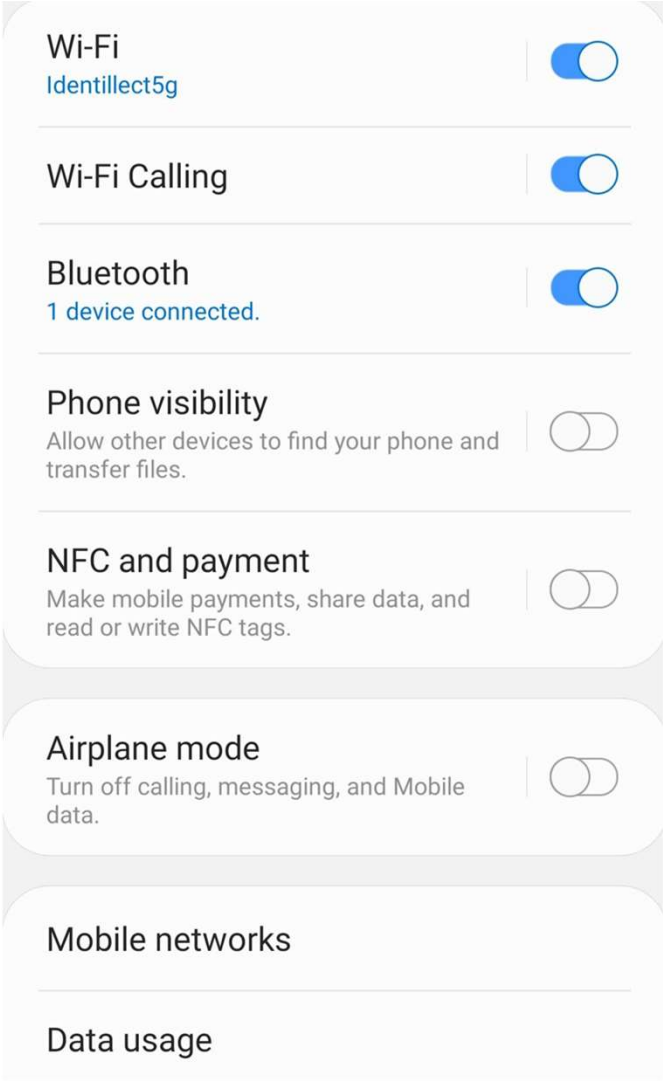
Turn Off Visibility

Turn on “hidden” mode and not “discoverable” mode

If previously paired, your devices will still pair when “hidden”

Why?

Cyber criminals have the capability to pair with your phone's open Bluetooth connection when you are not using it and steal personal information.

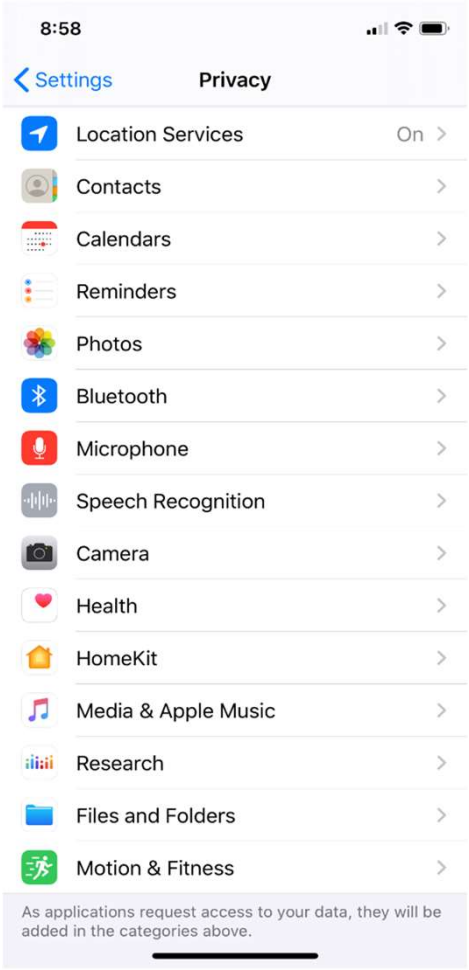


Mobile Device Charging

Avoid connecting your smartphone to any computer or charging station that you do not control
Example: Airport, hotel, library

Why?

- Connecting a mobile device to a computer using a USB cable can allow software running on that computer to interact with the phone in ways you may not anticipate.

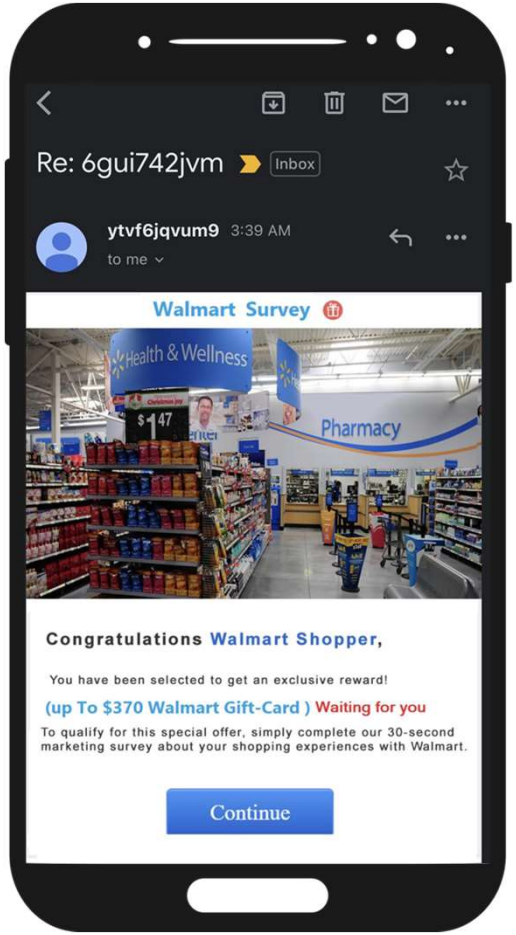


App Security & Privacy

- Ensure your installed apps only have access to the necessary information
- Remove access to unnecessary information
- Pay attention to apps that have access to your contacts, camera, location and microphone
- Limit location permissions
- Keep apps up to date, enable automatic updates
- Avoid using your social media profiles to log into apps

Mobile Ad Fraud

- Estimates on how much ad fraud costs vary, but Juniper Research projects a $100 billion loss per year by 2023
- Ad fraud can take several forms, but the most common is using malware to generate clicks on ads that appear to be coming from a legitimate user using a legitimate app or website.
- The biggest victims are mobile advertisers and ad-supported publishers, but ad fraud does harm to mobile users, too.
- Android is by far the most popular platform for mobile ad fraud. According to Upstream, these some of the most popular Android malicious apps to avoid:
- Snaptube, GPS Speedometer, Easy Scanner, Weather Forecast, Super Calculator, VidMate, Quicktouch



THANKS!

Do you have any questions?

Todd Sexton, MBA
Cyber Security Expert & CEO, Identillect Technologies

Email Address
todd@identillect.com

Phone Number
(888) 781-4080

IDENTILLECT TECHNOLOGIES

Danielle Cox is the Chief Information Security Officer with West Virginia's Office of Technology, where she manages the State's Security Operations Center, directs the Risk management and vulnerability program, and identifies other risks to State data, personnel, applications, and systems. Additionally, she trains, plans, and implements cyber security education throughout the State's enterprise. She has been a member of the Cybersecurity Team for 9 years.

Ms. Cox has an additional 12 years' experience as a Training Coordinator in the legal industry, helping end users take full advantage of available resources. She holds a BA with honors in Business Administration and Computer Information Systems from the University of Charleston, and a Masters in Technology Management and Information Security from Marshall University. Ms. Cox holds certifications as a Certified Information Systems Security Professional (CISSP), a GIAC Systems and Network Auditor Specialist (GSNA), and a Global Information Assurance Critical Controls Certification (GCCC). She is active in her community, volunteers regularly, and participates in raising service dogs for veterans.

Cybersecurity Essentials

MAKING YOUSELF LESS OF A TARGET

Cybersecurity Office
WV Office of Technology

Agenda

- Why do we exist?
- Securing Communications
- COVID Scams and Other New Threats
- Resurgence of Old Threats - Ransomware
- Other Considerations for Government Entities
- Questions and Answers

Welcome

CSO

STATE GOVERNMENT

CRITICAL INFRASTRUCTURE

CYBER WORKFORCE

CYBER RISK

CYBER OUTREACH

CYBER PROTECTION

CYBER OPERATIONS

ENGAGE

EDUCATE

ADAPT

ACT

“ We all have a fear of the unknown. What one does with that fear will make all the difference in the world.”

Lillian Russell

THREAT LANDSCAPE

What are we up against?

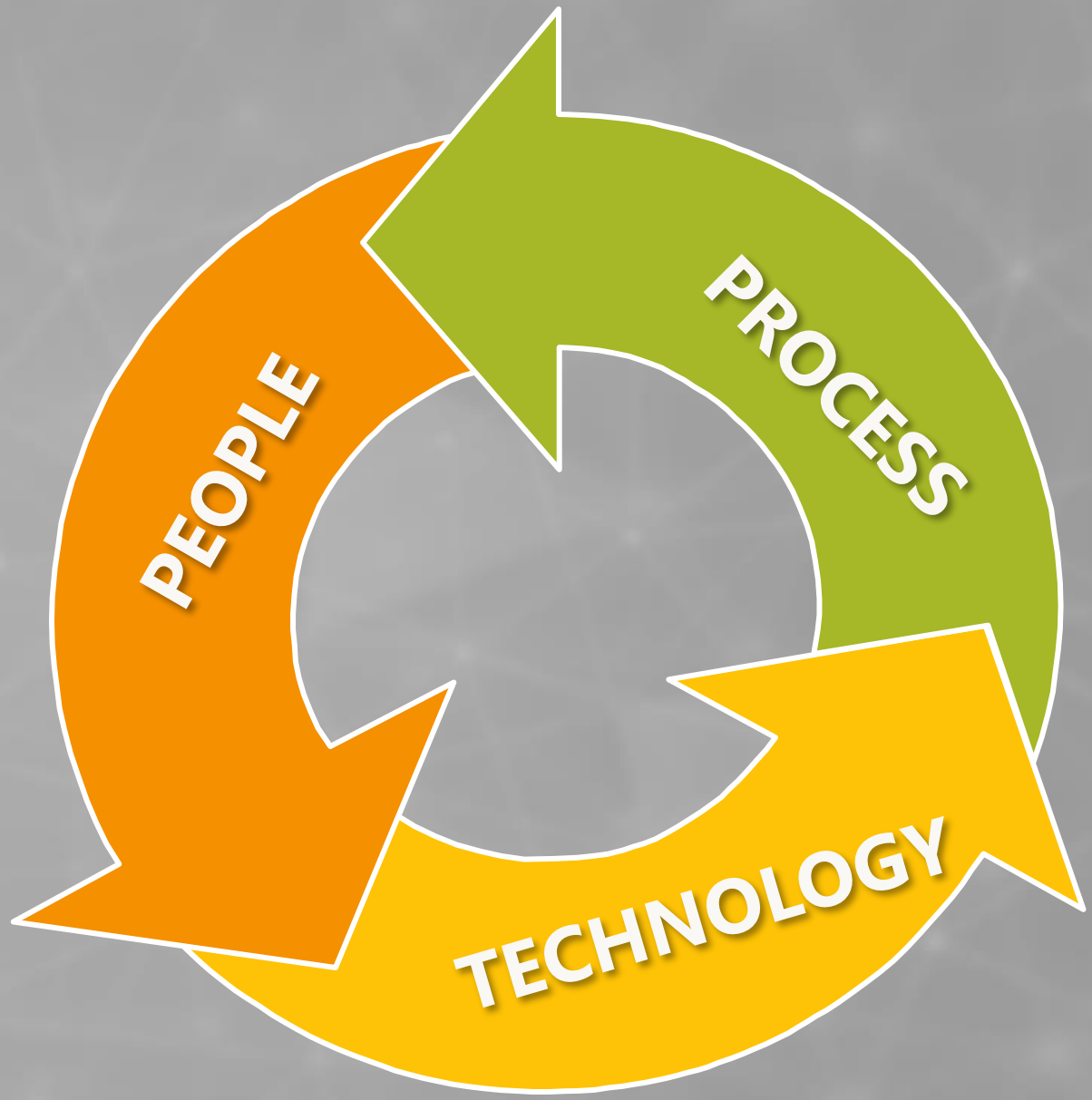
Outnumbered, underfunded, stretched thin

Cyber Security

Think in Threes

Confidentiality
Availability
Integrity

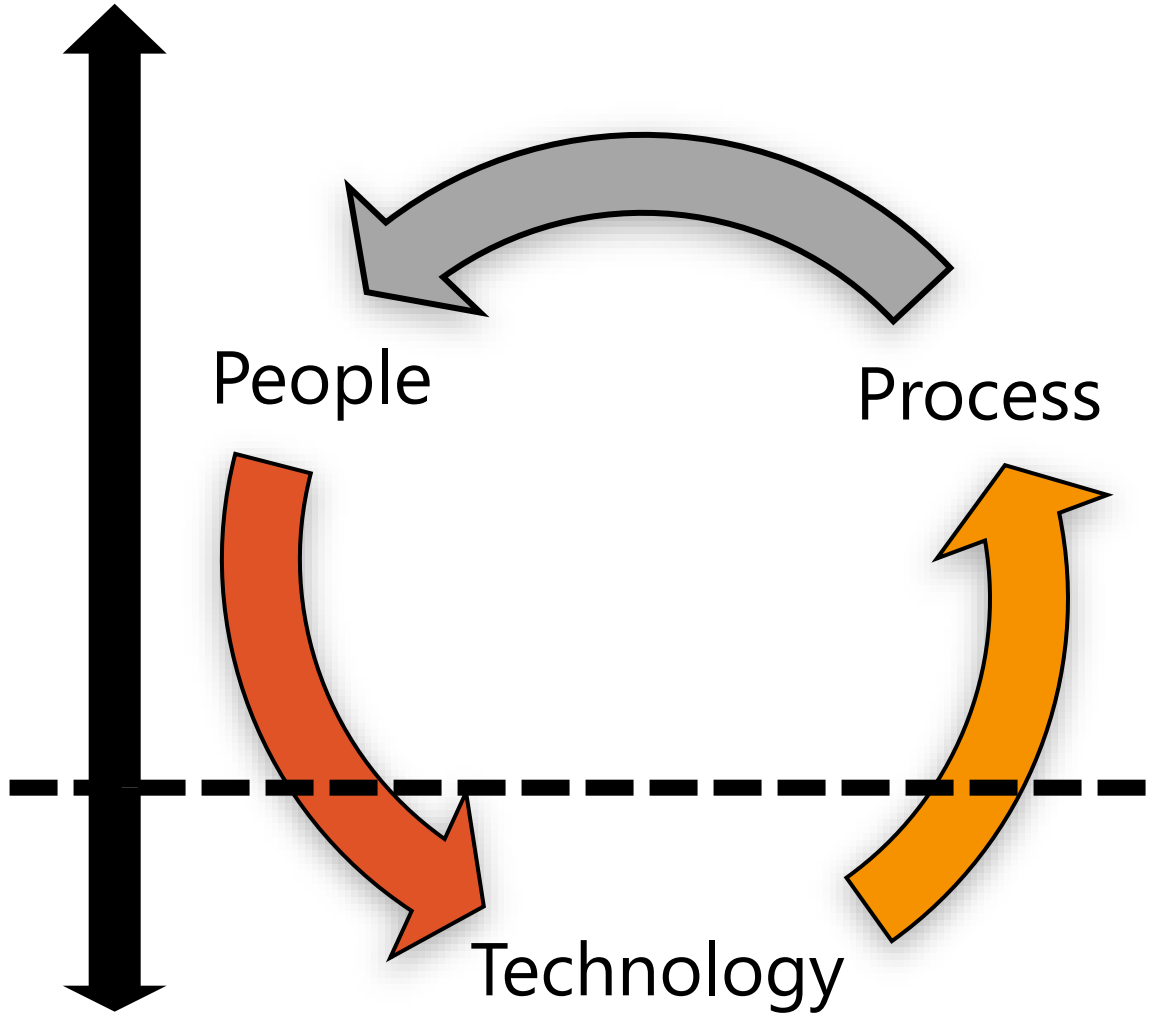
People
Process
Technology



90/10 Rule

90% of security safeguards rely on the computer user to adhere to good computing practices

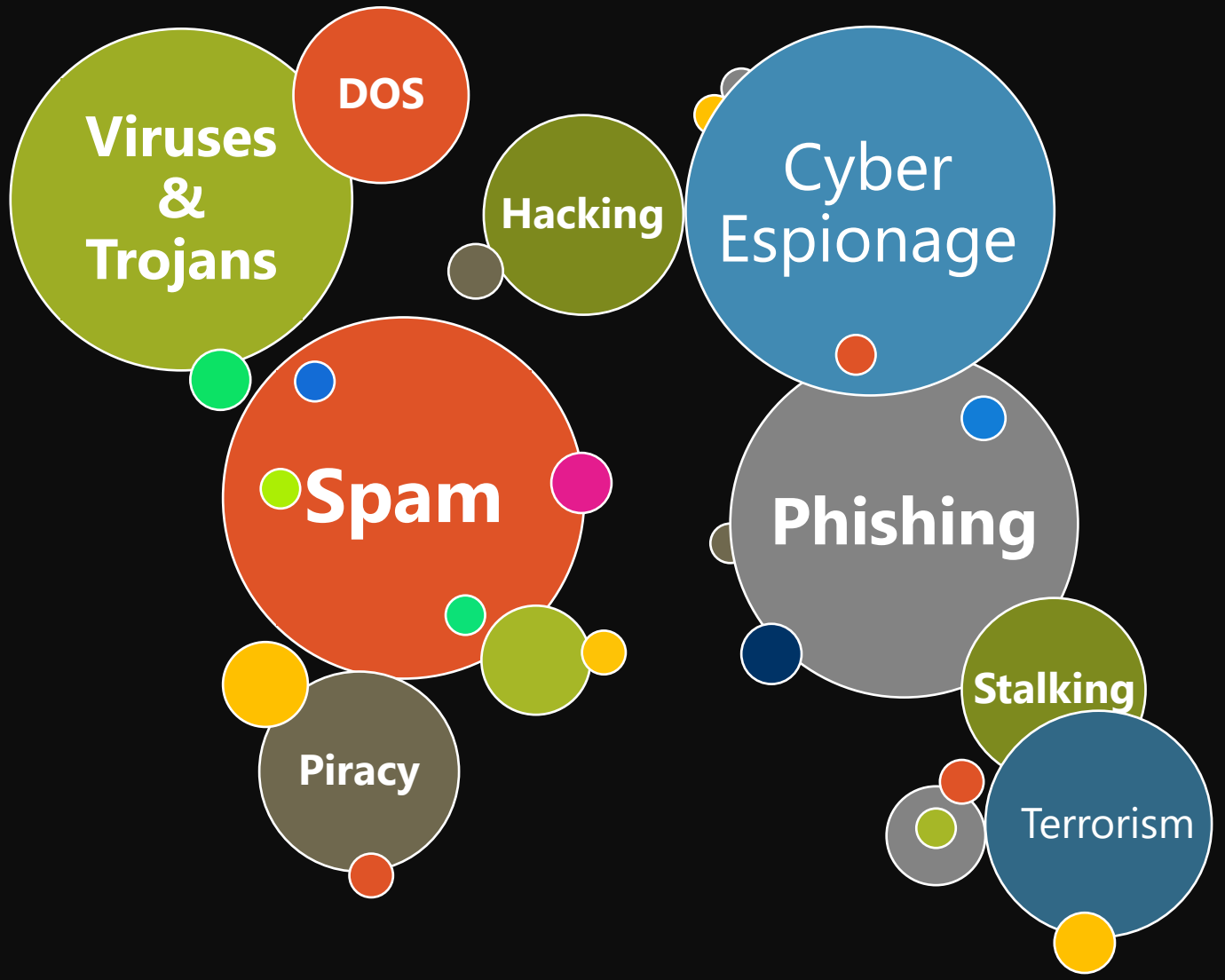
10% of security safeguards are technical



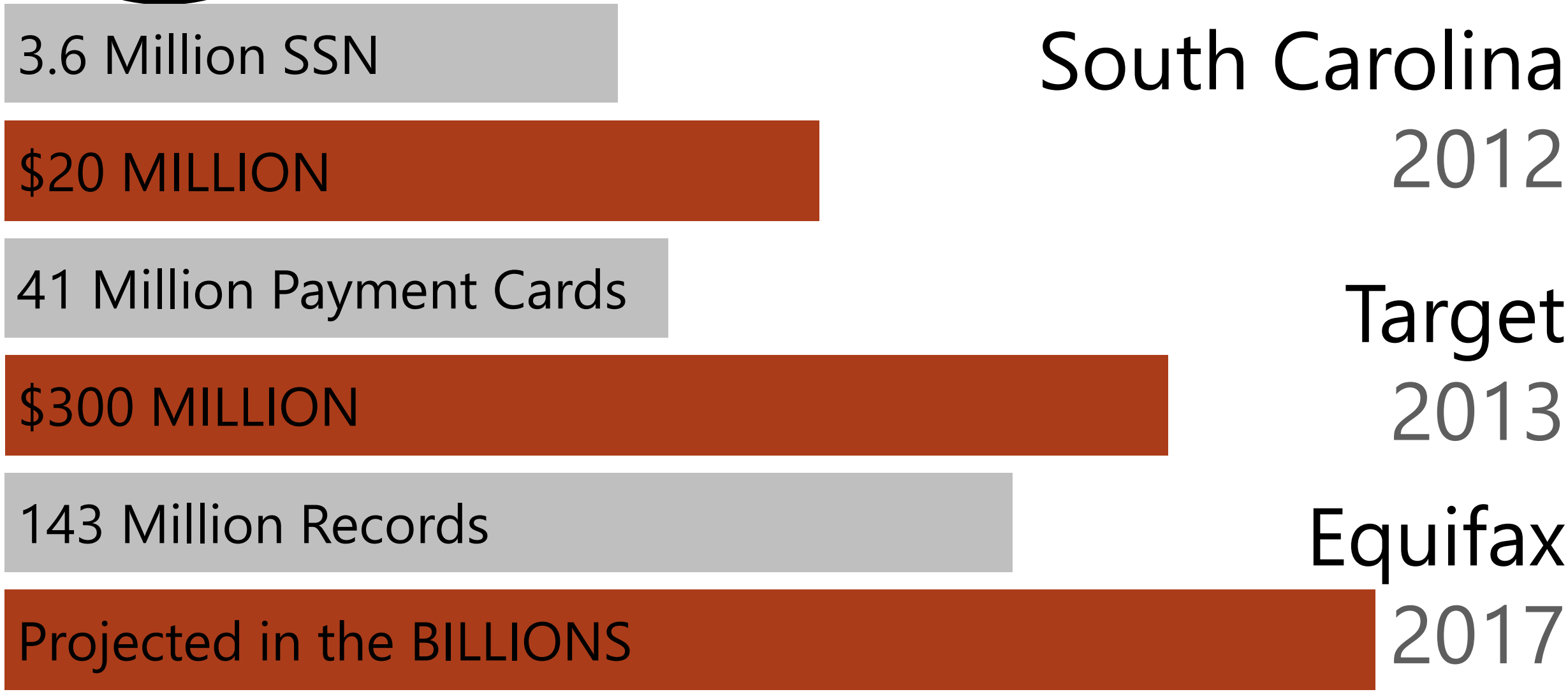
Bad Guys

Who does what?

- Hackers
- Crackers
- Malware Writers
- Phreakers
- Cyber Terrorists
- Cyber Scammers



Cost of a Data Breach



IoT

Smart devices

Not just home automation

Printers, hard drives, HVAC, etc.

SEC Consult

Home Portfolio Vulnerability Lab Blog Career About us Contact

MULTIPLE CRITICAL VULNERABILITIES IN VIBRATISSIMO SMART SEX TOY PRODUCT RANGE

The sex toys of the "Vibratissimo" product line and their cloud platform, both manufactured and operated by the German company Amor Gummiwaren GmbH, were affected by severe security vulnerabilities. The database containing all the customer data (explicit images, chat logs, sexual orientation, email addresses, passwords in clear text, etc.) was basically readable for everyone on the Internet. Moreover, an attacker was able to remotely pleasure individuals without their consent. This could be possible if an attacker is nearby a victim (within Bluetooth range), or even over the Internet. Furthermore, the enumeration of explicit images of all users is possible because of predictable numbers and missing authorization checks.

VENDOR DESCRIPTION

"Control with Vibratissimo your AMOR Toy on your smartphone and get even more features by the app. With Vibr
and exciting opportunities, whether you are in the same room or on different continents."

Source: http://www.vibratissimo.com/en/index.html

BUSINESS RECOMMENDATION

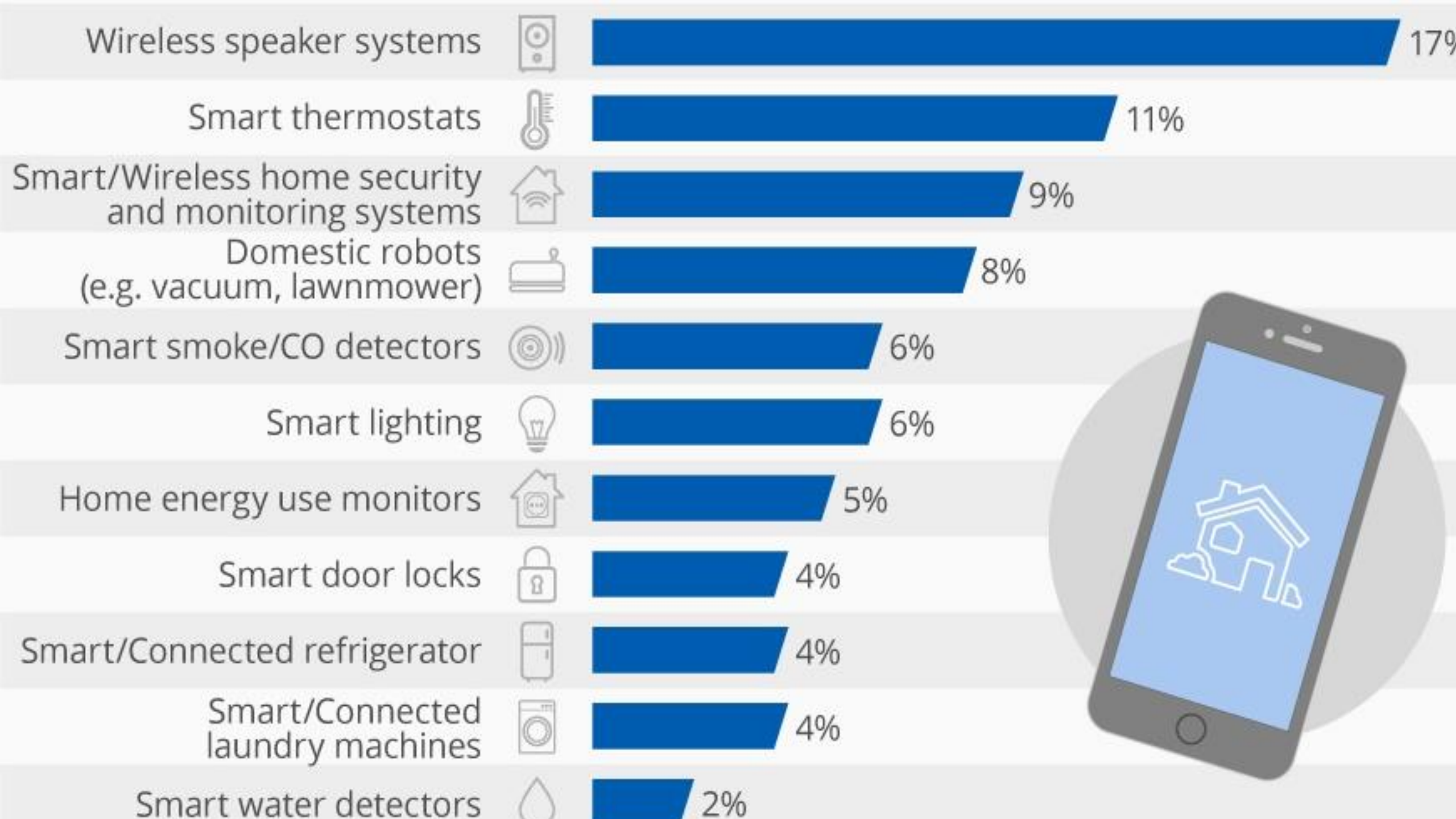
SEC Consult highly recommends to update the app to the newest version available in the appstore. Furthermor
used within the app, should be changed immediately. If the password was used for multiple services, all passw
rid of issue number 3 (Unauthenticated Bluetooth LE Connections) a firmware update can be applied. To apply
devices have to be sent to Amor Gummiwaren GmbH.

TITLE
Multiple critical vulnerabilities

PRODUCT
Whole Vibratissimo Smart Sex range

FOUND

Explicit images, chat logs, sexual orientation, email addresses, and passwords were available to everyone on the Internet.

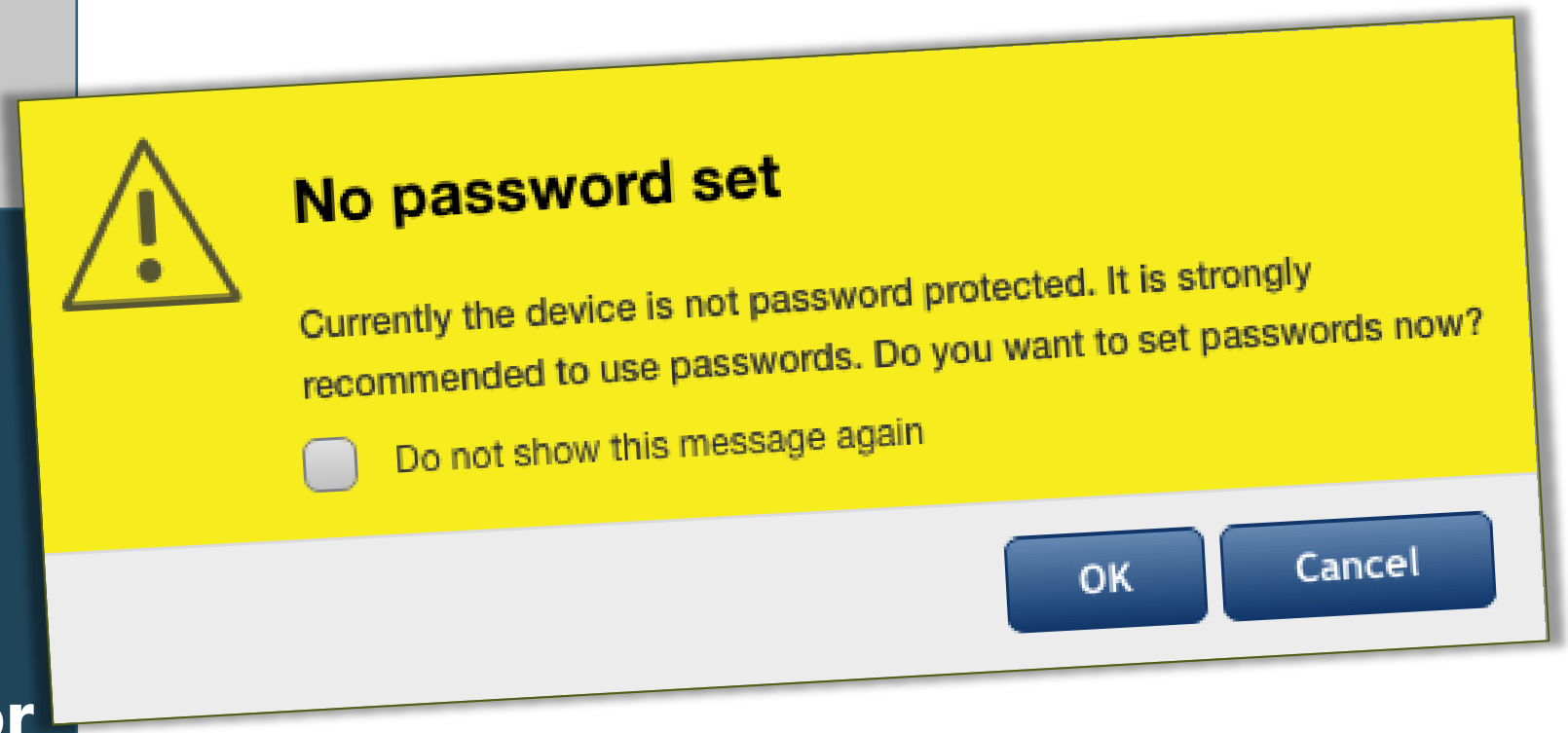

Wireless speaker systems
17%
Smart thermostats
11%
Smart/Wireless home security and monitoring systems
9%
Domestic robots (e.g. vacuum, lawnmower)
8%
Smart smoke/CO detectors
6%
Smart lighting
6%
Home energy use monitors
5%
Smart door locks
4%
Smart/Connected refrigerator
4%
Smart/Connected laundry machines
4%
Smart water detectors
2%

Default passwords

More common than you'd think

Unless you manually change the password this is standard behavior on many devices

Internet facing devices need special care

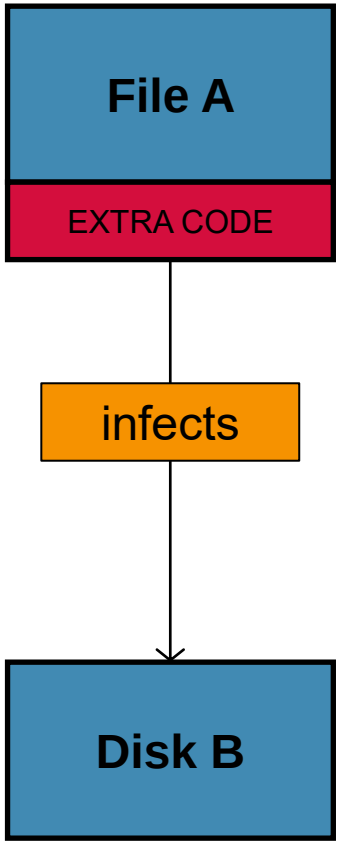


CHALLENGES

So much to do, so little resources…so many silly users

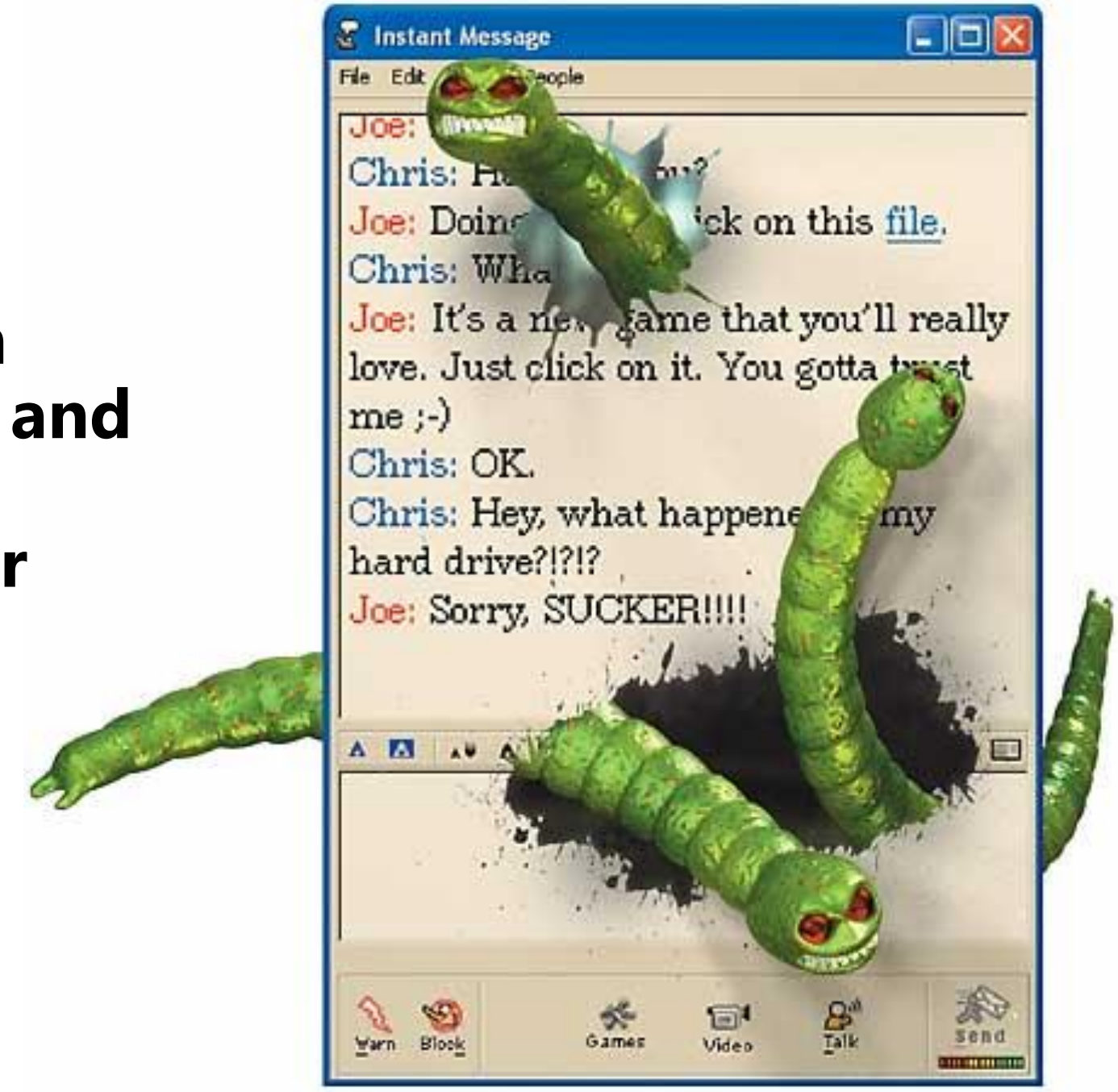
Virus

- A virus attaches itself to a program, file, or disk
- When the program is executed, the virus activates and replicates itself
- The virus may be benign or malignant but executes its payload at some point



Worm

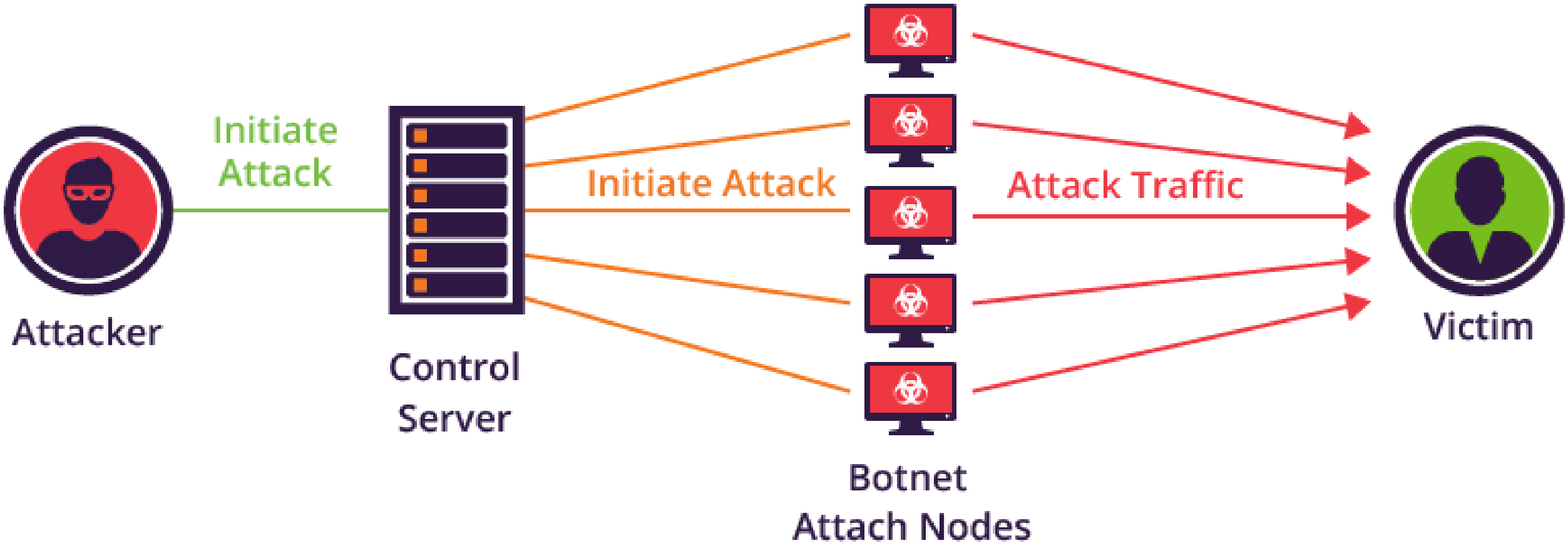
Independent program which replicates itself and sends copies from computer to computer across network connections.



OTHERS

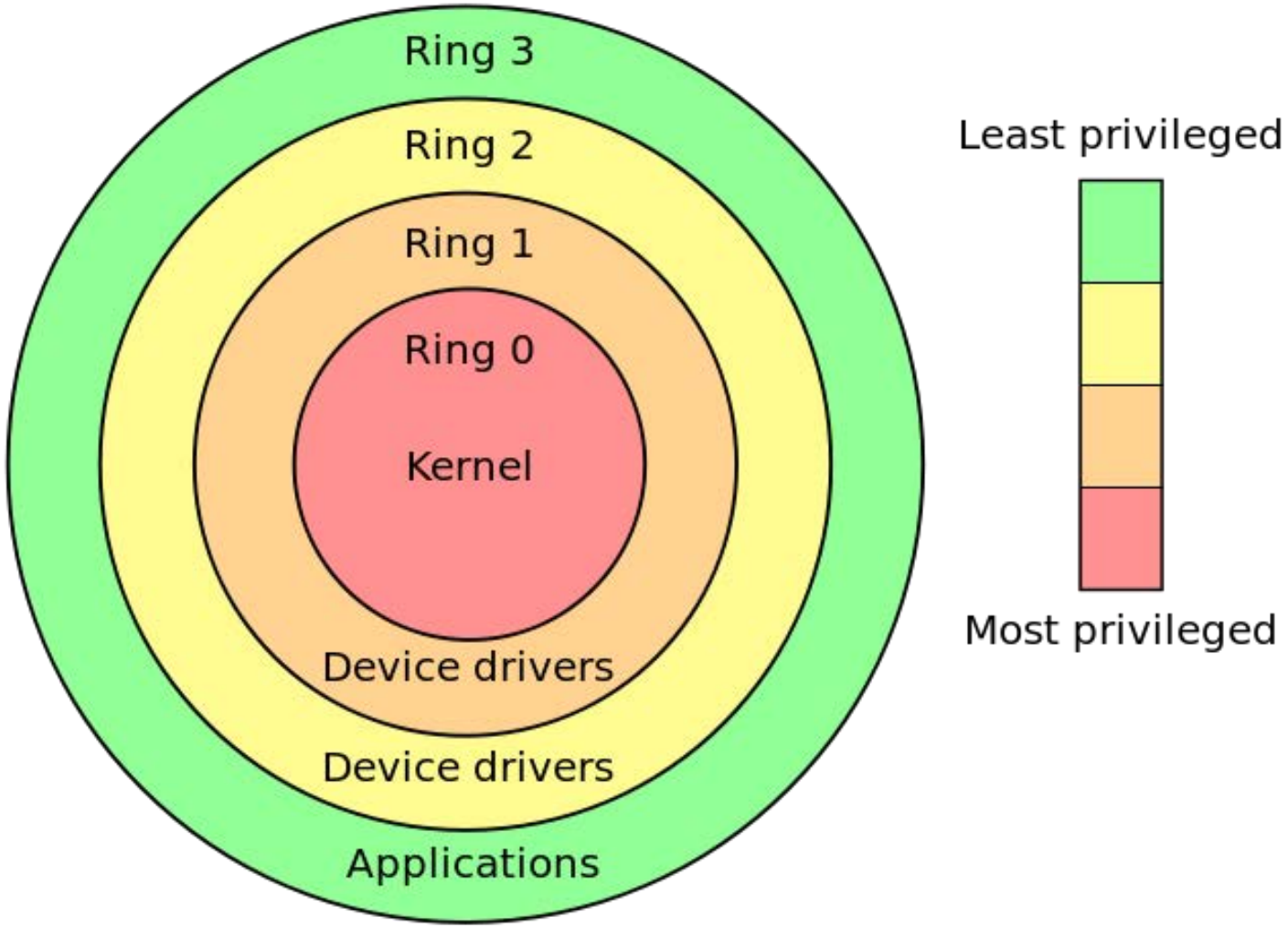
- Logic Bomb: Malware logic executes upon certain conditions. Program is often used for legitimate reasons.
- Trojan Horse: Masquerades as beneficial program while quietly destroying data or damaging your system.

Botnet


Initiate
Attack
Attacker
Control
Server
Initiate Attack
Botnet
Attach Nodes
Attack Traffic
Victim

Rootkit

- Upon penetrating a computer, a hacker installs a collection of programs, called a rootkit
- Eliminates evidence of break-in
- Modifies the operating system



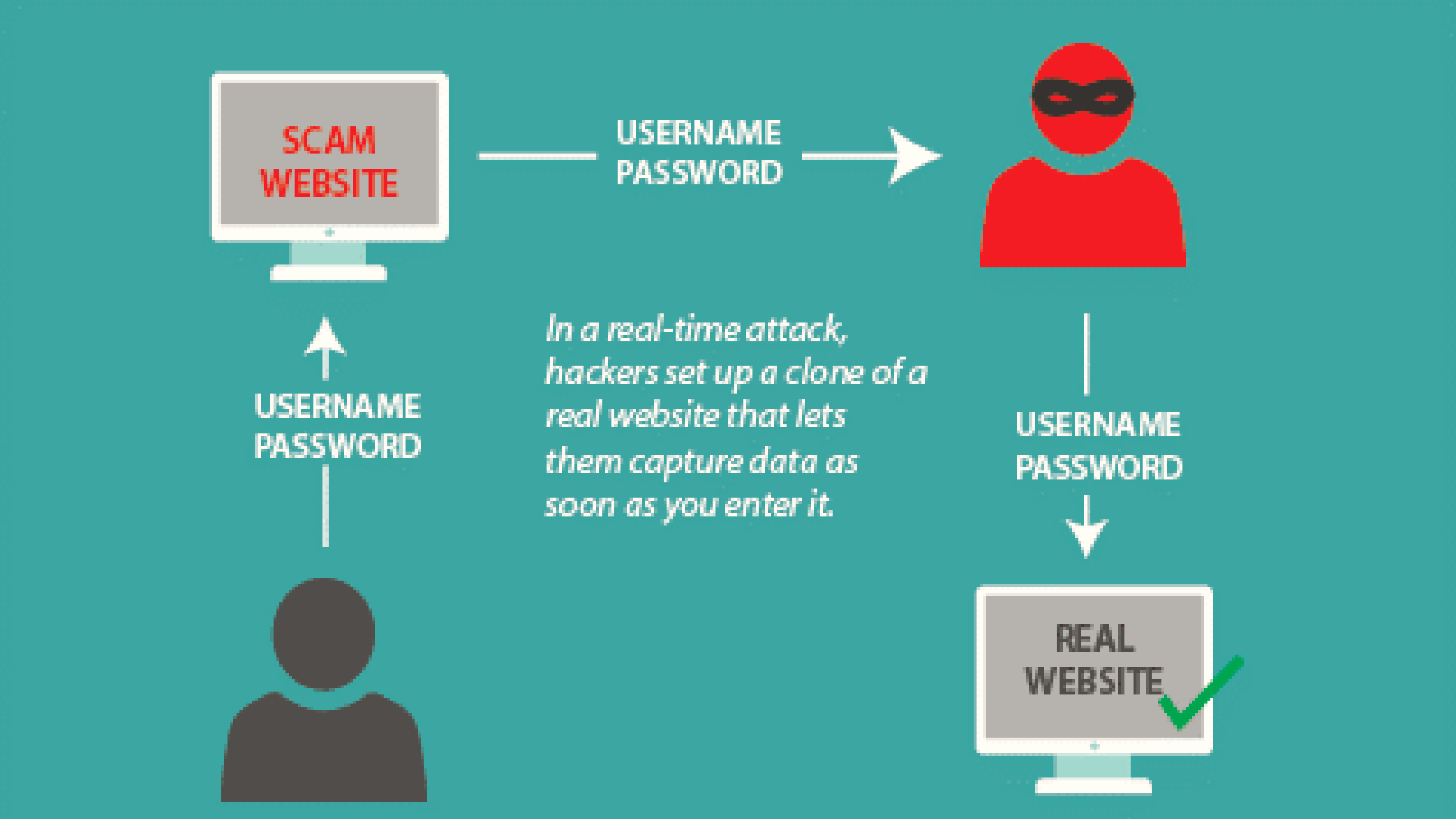
Social Engineering

SCAMS

Phishing

Vishing

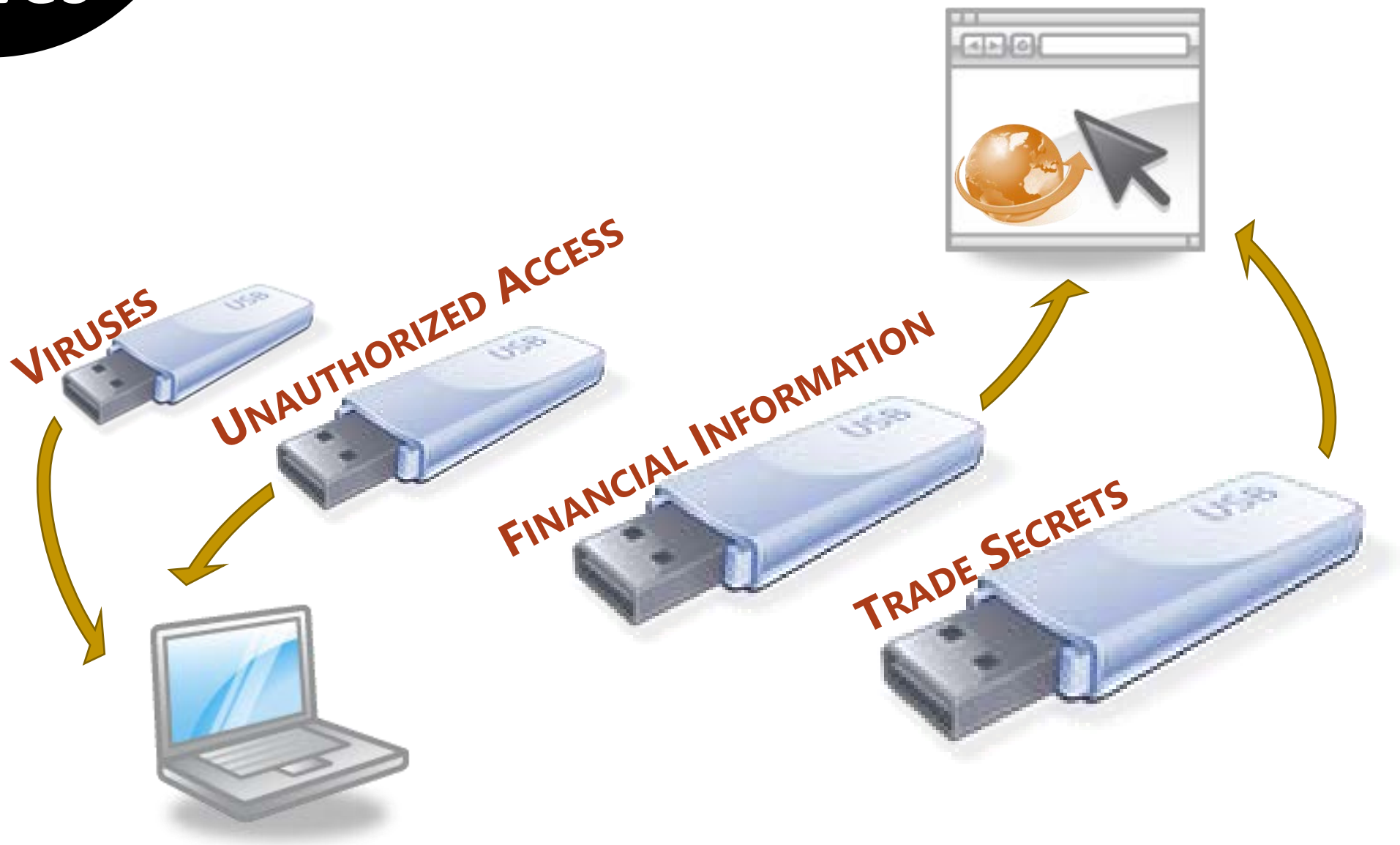
Smishing


SCAM WEBSITE
USERNAME PASSWORD
USERNAME PASSWORD
In a real-time attack, hackers set up a clone of a real website that lets them capture data as soon as you enter it.
USERNAME PASSWORD
REAL WEBSITE

Physical

- Vehicles
- Coffee shops
- Your office
- Their office
- Hotels
- Airports
- Libraries
- Court

Thumb Drives



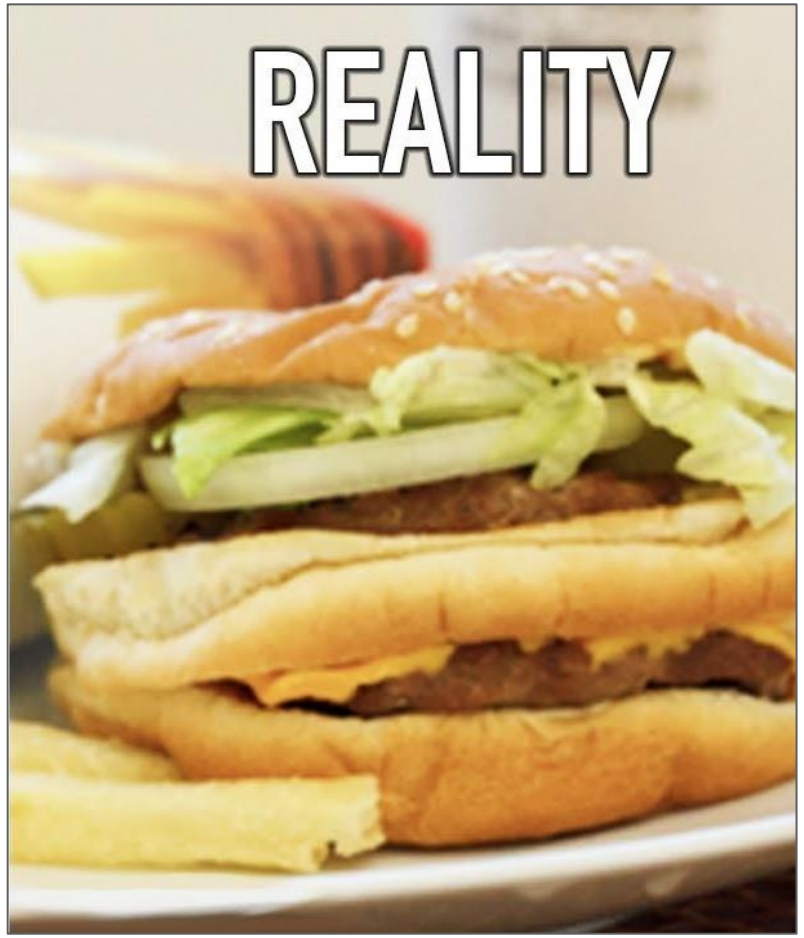
Portable Storage

External Hard Drives
Mobile Devices
CDs
DVDs
Floppy Disks
Cameras

HOW TO FIX THIS?

Minimum

- Establish Cyber Security as a critical issue;
- Establish Cyber Security is Technical AND Business issue; and
- Cyber Risk Management is best approach.



What people expect,
What you work with

- Citizens expect government services to be as competitive as the largest tech companies.
- Google, Microsoft, Apple have many more resources.
- If quality services aren't available they will use third party ones that get the job done.

Updating Software

Regularly install updates

Subscribe to automatic software updates whenever they are offered

Example: You can automatically update all Microsoft software.

Uninstall software that you don't use.

Malware Defense

Use it and update it.

Shop Safely Online

Check Reviews

Third-party Seals of Approval.

Website Protects Data:

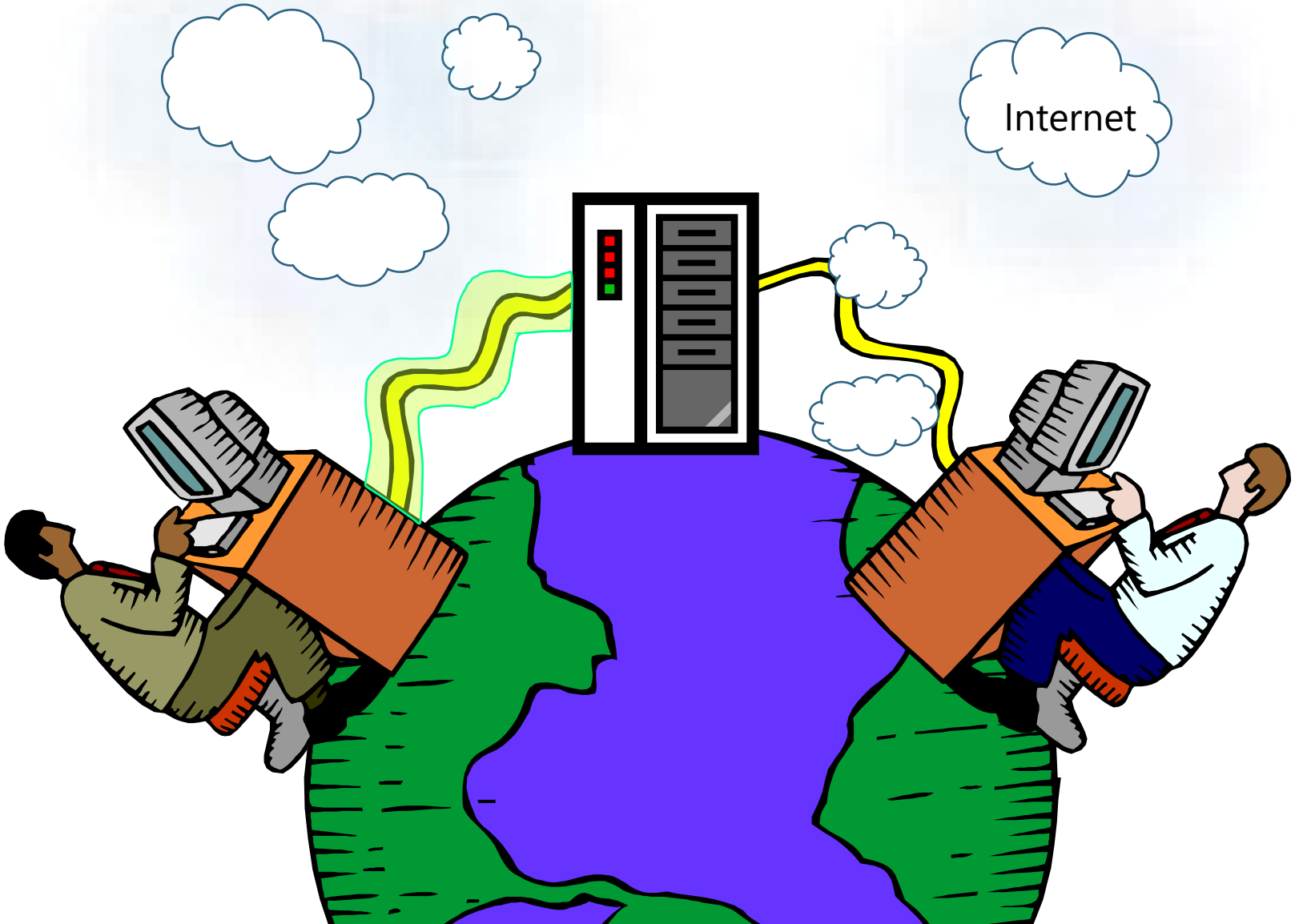
HTTPS

Padlocks

Use a Filter

Keep Web Browser Updated

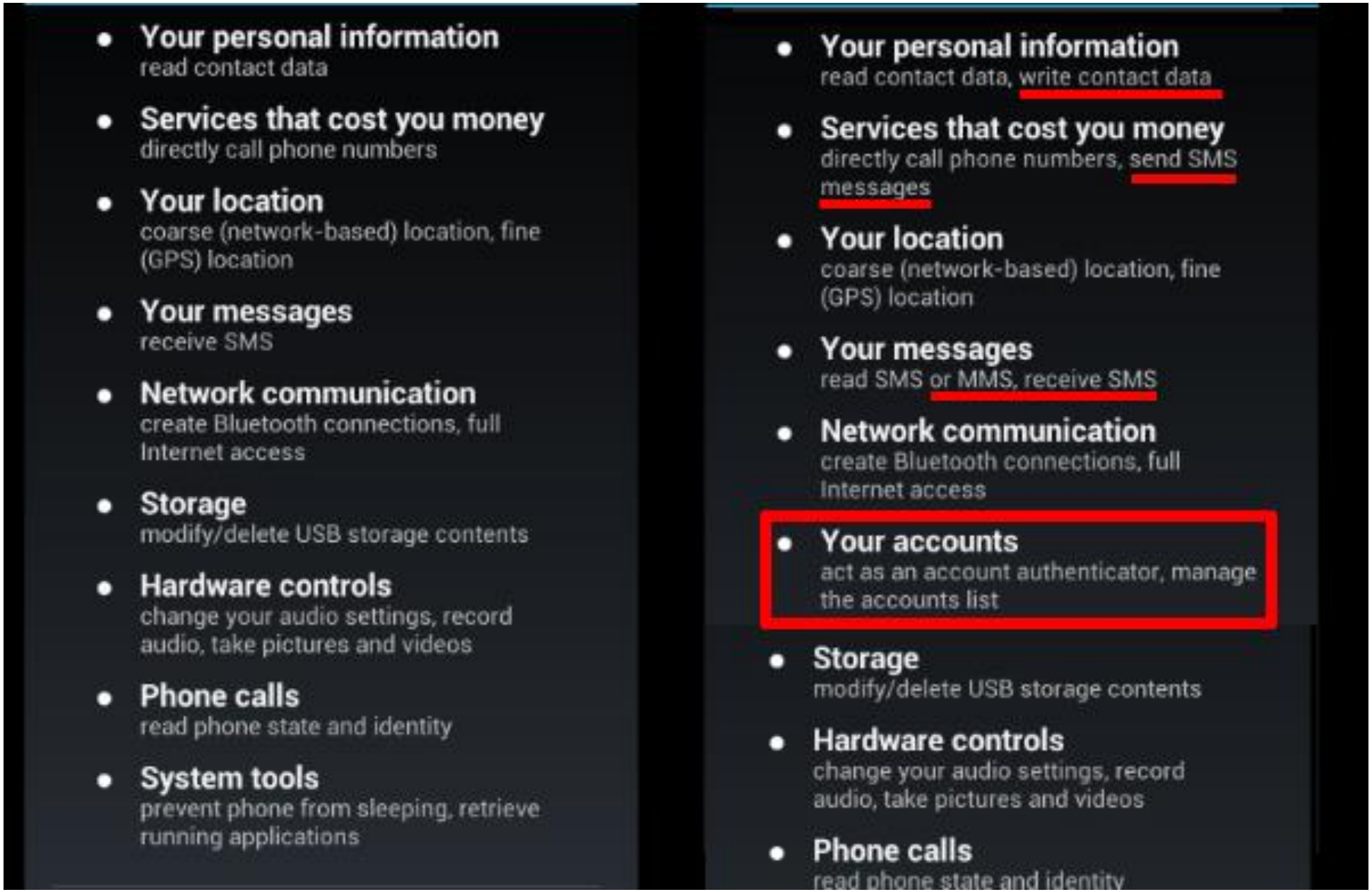
VPN



Securing Email

- Sender's Computer
- Sender's Mail Server
- Internet
- Each Recipient's Mail Server
- Each Recipient's Computer

Apps


Your personal information
read contact data
Services that cost you money
directly call phone numbers
Your location
coarse (network-based) location, fine (GPS) location
Your messages
receive SMS
Network communication
create Bluetooth connections, full Internet access
Storage
modify/delete USB storage contents
Hardware controls
change your audio settings, record audio, take pictures and videos
Phone calls
read phone state and identity
System tools
prevent phone from sleeping, retrieve running applications
Your personal information
read contact data, write contact data
Services that cost you money
directly call phone numbers, send SMS messages
Your location
coarse (network-based) location, fine (GPS) location
Your messages
read SMS or MMS, receive SMS
Network communication
create Bluetooth connections, full Internet access
Your accounts
act as an account authenticator, manage the accounts list
Storage
modify/delete USB storage contents
Hardware controls
change your audio settings, record audio, take pictures and videos
Phone calls
read phone state and identity

MFA

- User is only granted access after presenting two or more factors of proof.
- Opt-in for modern services
- Can be added to most systems
- MFA drawbacks

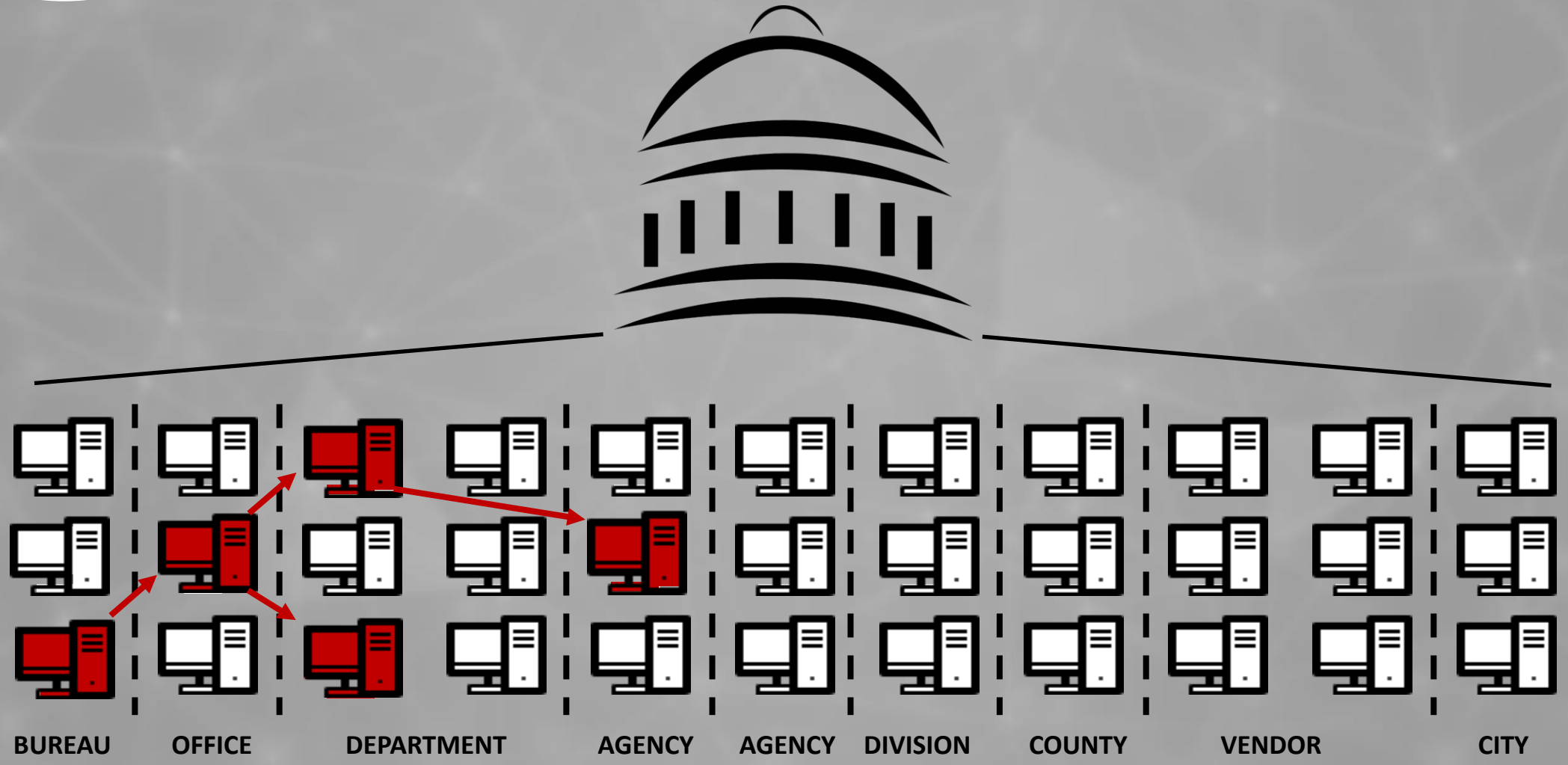
WHEN YOU WANT TO GET SERIOUS

How much do you know about your data?

Who is currently making risk decisions?

Is the organization emphasizing PROACTIVE Privacy & Cyber Security?

UNDOCUMENTED SHARED RISK



SECURITY: DEFENSE IN DEPTH

Data

Application

Host

Internal Network

Perimeter

Policies and Procedures

Physical

Insecure Configurations

NIST, DISA, CIS vs. Business Needs
Builds
System Upgrades
Vulnerability Scans

Note: Federal Student Aid Secure Configuration Guides are based off the NIST checklist located at http://checklists.nist.gov


OOPS!

accountability

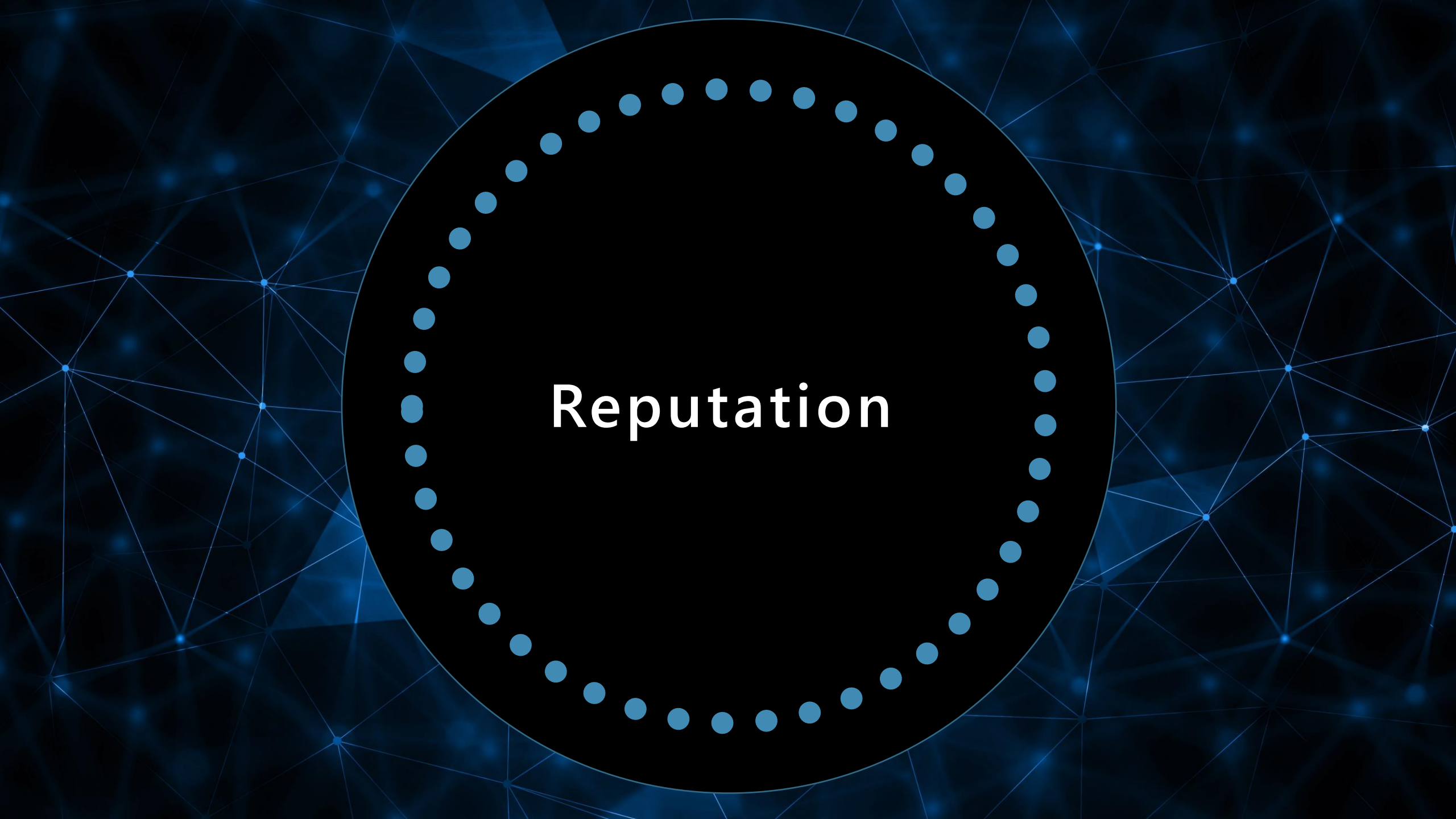
Holds individual responsible for actions taken

Logging, cameras

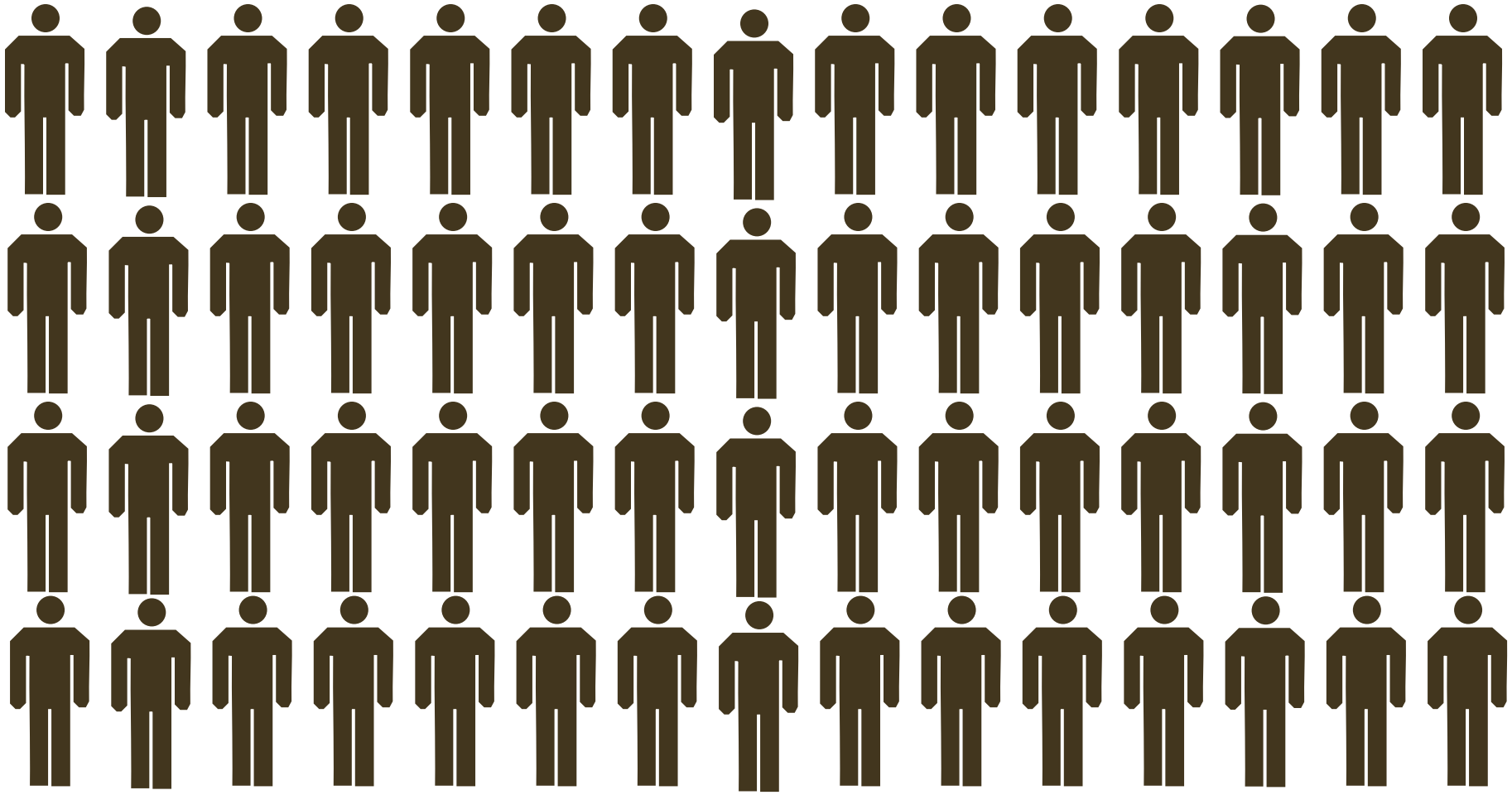
Consequences are needed for accountability

Incidents

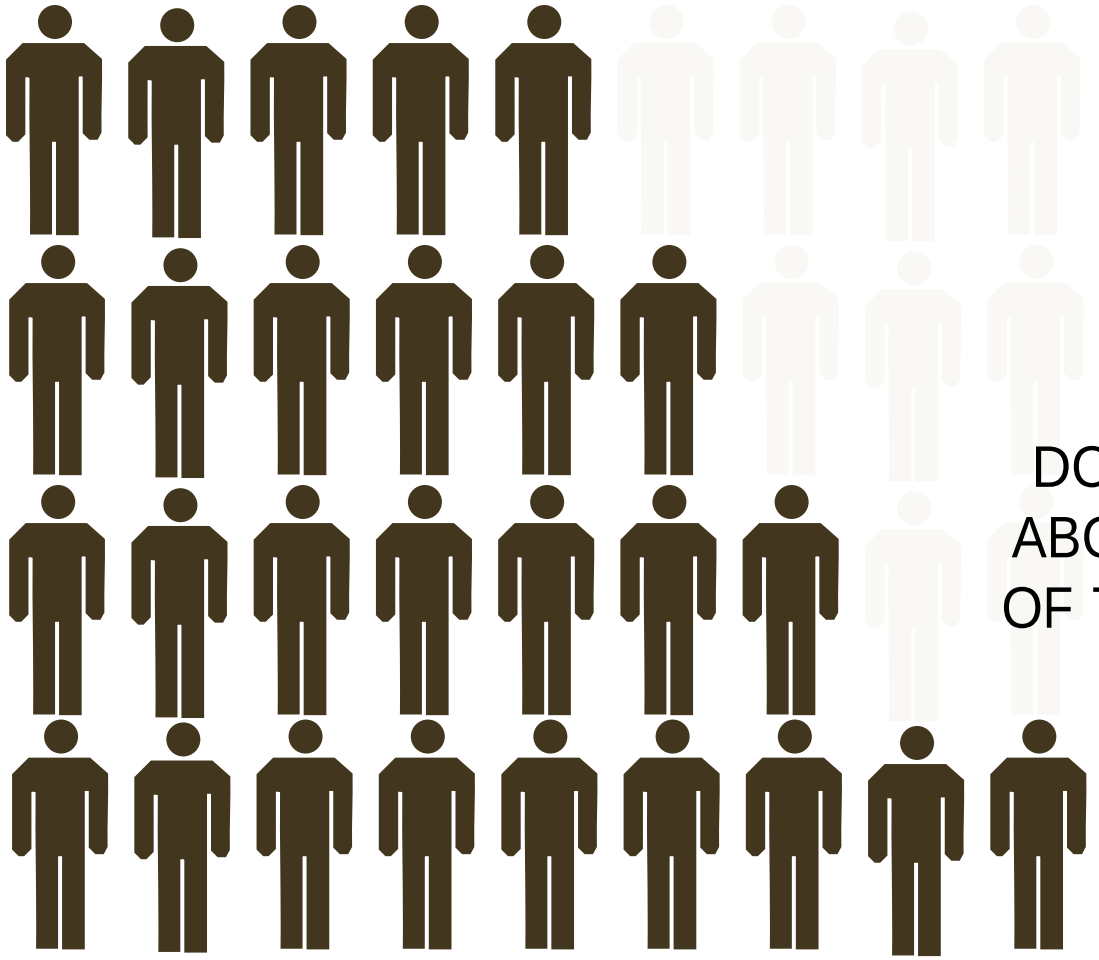

Identify
LEARN
LEARN
Prevent
Incident Management
Analyse
LEARN
LEARN
Correct


Reputation

It Matters



It Matters



56%

DO NOT ACTIVELY THINK
ABOUT THE CONSEQUENCE
OF THEIR ONLINE ACTIONS

It Matters

21%

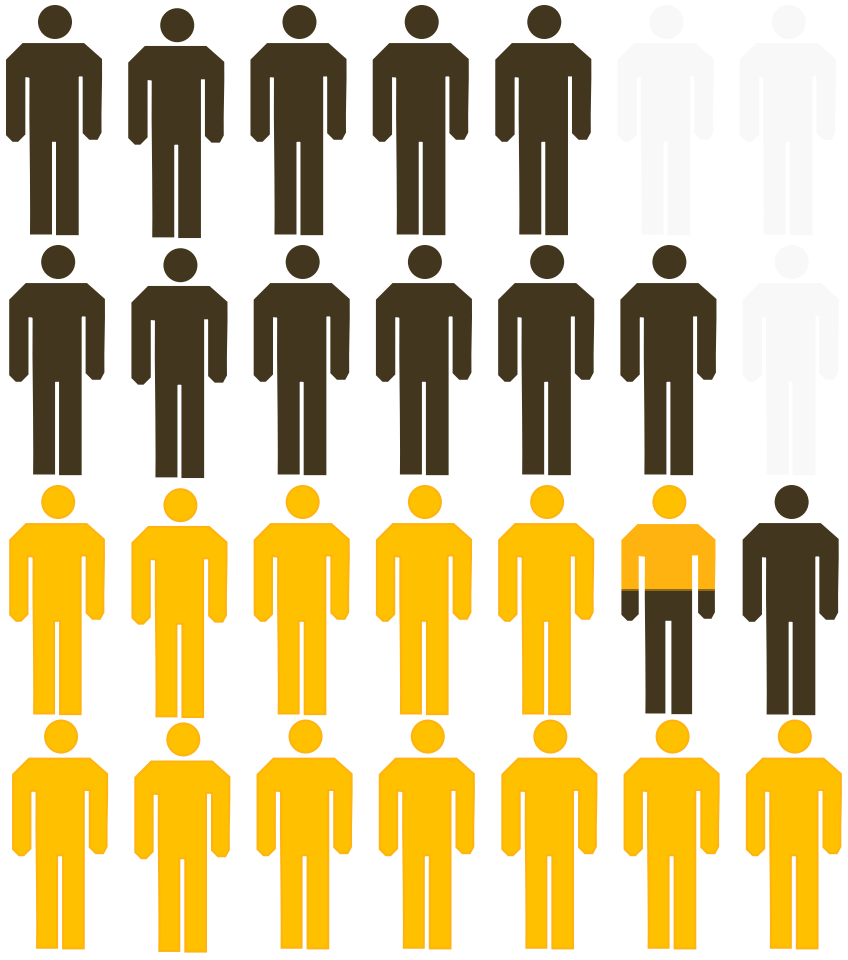
WERE FIRED
FROM A JOB

It Matters

16%

LOST OUT ON
GETTING A JOB

It Matters



16%

LOST THEIR
HEALTH INSURANCE

It Matters

14%

LOST OUT ON
A COLLEGE
THEY WANTED

It Matters

Protect Yourself

Simple Steps

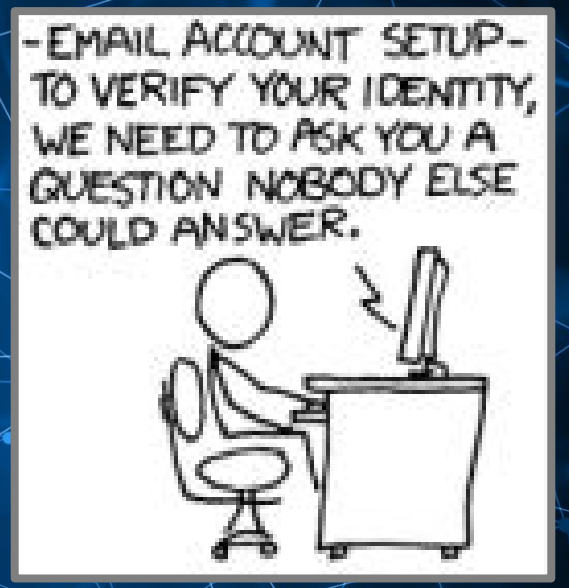
Birth Info

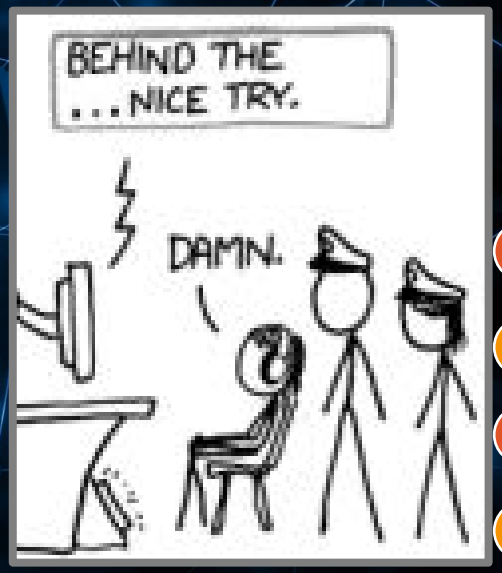
Protect Yourself

Simple Steps

Birth Info

Security Questions





Protect Yourself

Simple Steps

Birth Info

Security Questions

Physical Address

Protect Yourself

Simple Steps

Birth Info

Security Questions

Physical Address

House Layout

Protect Yourself

Simple Steps

Birth Info

Security Questions

Physical Address

House Layout

Vacations

Protect Yourself

Simple Steps

- Birth Info
- Security Questions
- Physical Address
- House Layout
- Vacations
- Confessionals

Protect Yourself

Simple Steps

- Birth Info
- Security Questions
- Physical Address
- House Layout
- Vacations
- Confessionals
- Phone Numbers

Protect Yourself

Simple Steps

- Birth Info
- Security Questions
- Physical Address
- House Layout
- Vacations
- Confessionals
- Phone Numbers
- Risky Behavior

DON’T

Inappropriate Photos

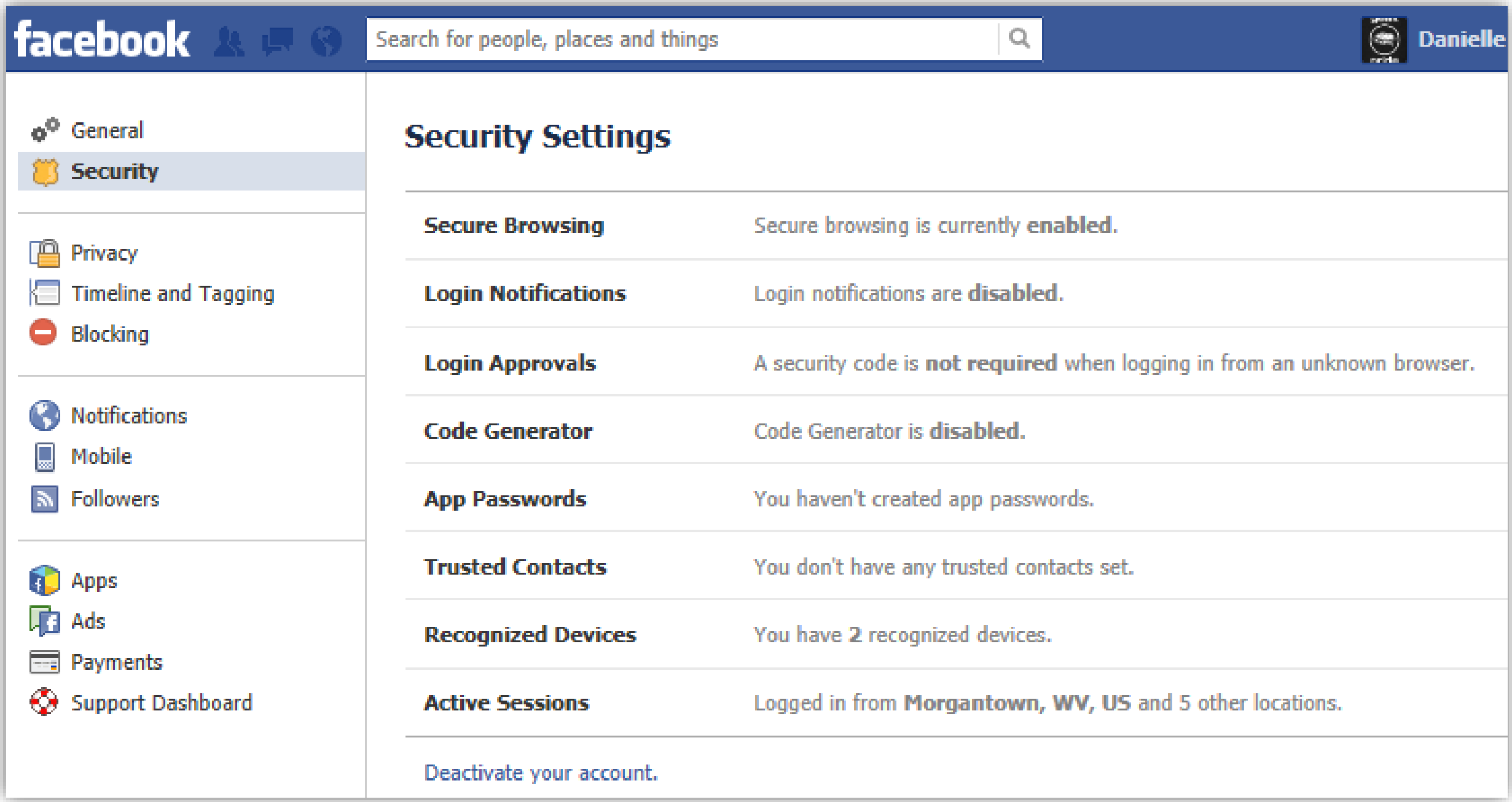
Drunken/Party

Sexual

Illegal

Demeaning

Discriminating


facebook
Search for people, places and things
Danielle
General
Security
Privacy
Timeline and Tagging
Blocking
Notifications
Mobile
Followers
Apps
Ads
Payments
Support Dashboard
Security Settings
Secure Browsing
Secure browsing is currently enabled.
Login Notifications
Login notifications are disabled.
Login Approvals
A security code is not required when logging in from an unknown browser.
Code Generator
Code Generator is disabled.
App Passwords
You haven't created app passwords.
Trusted Contacts
You don't have any trusted contacts set.
Recognized Devices
You have 2 recognized devices.
Active Sessions
Logged in from Morgantown, WV, US and 5 other locations.
Deactivate your account.

Stay on Top of Things

Search for yourself/organization

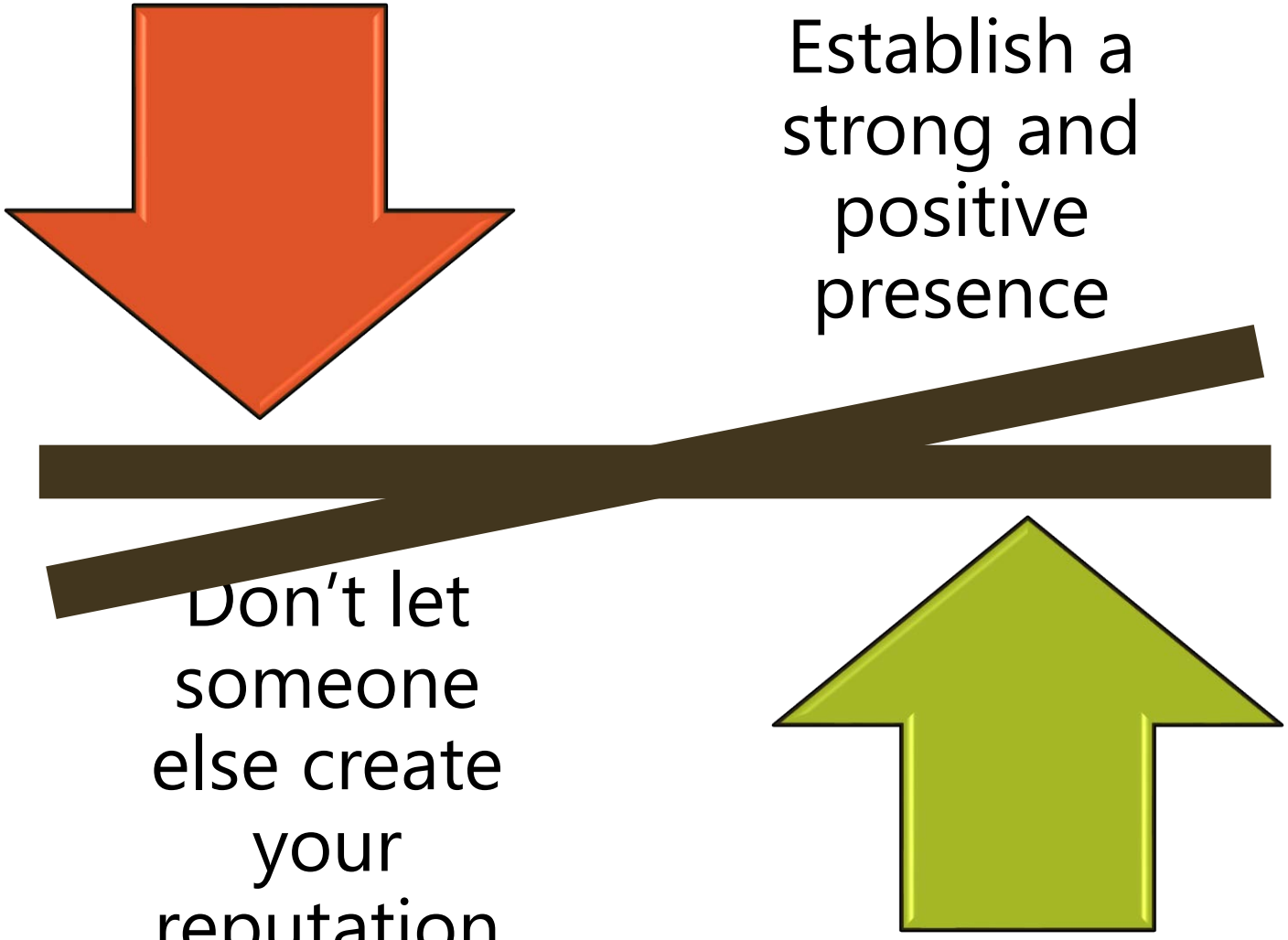
Setup alerts

Check aliases

Check other's social media

- Assess
- Acknowledge
- Delete
- Push
- Promote

Set Your Own Reputation



IN SUMMARY

- Make risk-based decisions from the top-down
- Know your environment, data, and resources
- Be prepared…Be prepared to learn from mistakes.

Questions?

THANK YOU

DANIELLE COX
Cyber Risk Manager
Cybersecurity Office
WV Office of Technology

Angie Volk is a graduate of the West Virginia University College of Law and was admitted to practice in West Virginia in 1994. She has previously worked as in-house counsel for Columbia Gas, as a law clerk for the Honorable Joseph R. Goodwin and as the CJA Supervising Attorney for the Southern District of West Virginia. She is currently the Compliance Coordinator at the West Virginia State Bar and handles CLE and membership matters.

Mike Mellace has been the Information Technology Directory at the West Virginia State Bar since 2012. He has a Bachelor's Degree from Marshall University in Management Information Systems and a Master's Degree from Marshall University in Technology Management. Mike has worked over the past 15 years in Education, Marketing and Legal organizations. As the IT Director, he has played a critical role in upgrading websites, databases, phone systems, and hardware internally at the State Bar Center.