Demystifying Cybersecurity

2019 AICPA Women’s Global Leadership Summit

Amber Welch

Cyber Risk Specialist at McKinsey

MA, CISSP, CISA, CIPP/E, CIPM, FIP, CCSK, ISO 27001 Lead Auditor

Twitter: @MsAmberWelch

LinkedIn: linkedin.com/in/amberwelch1

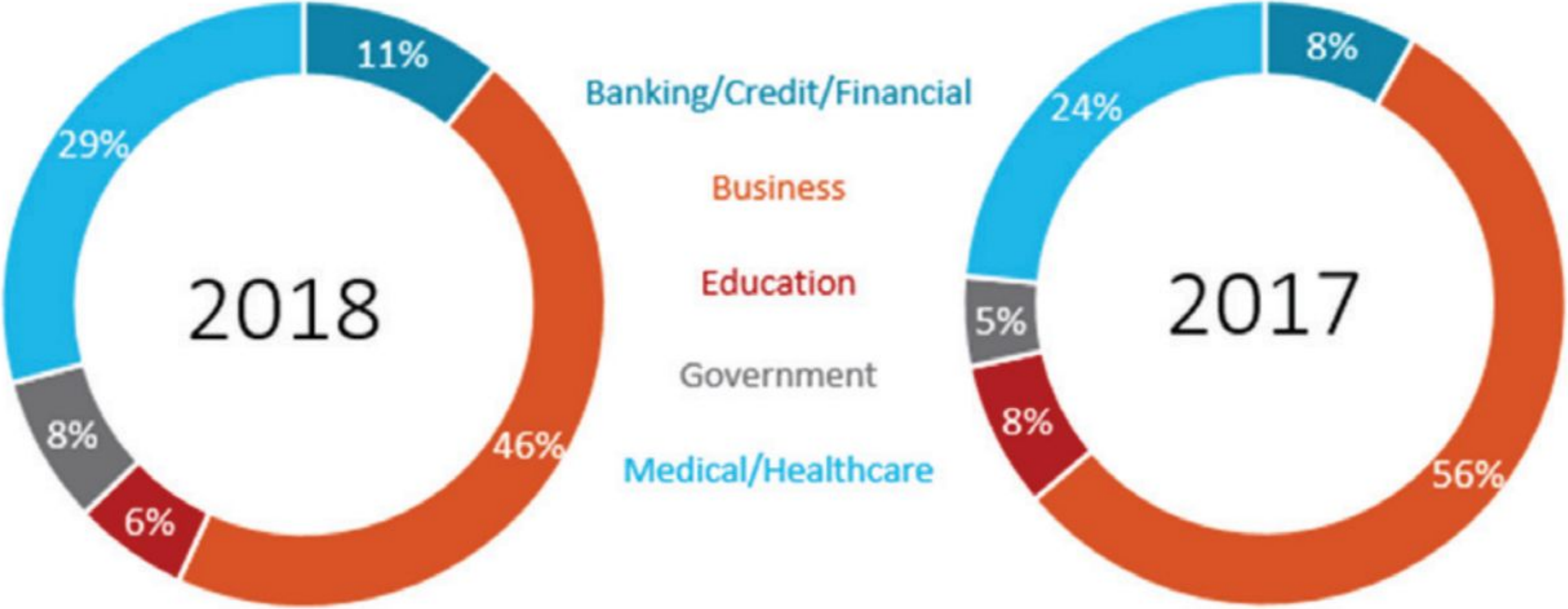
GitHub: github.com/MsAmberWelch

Agenda

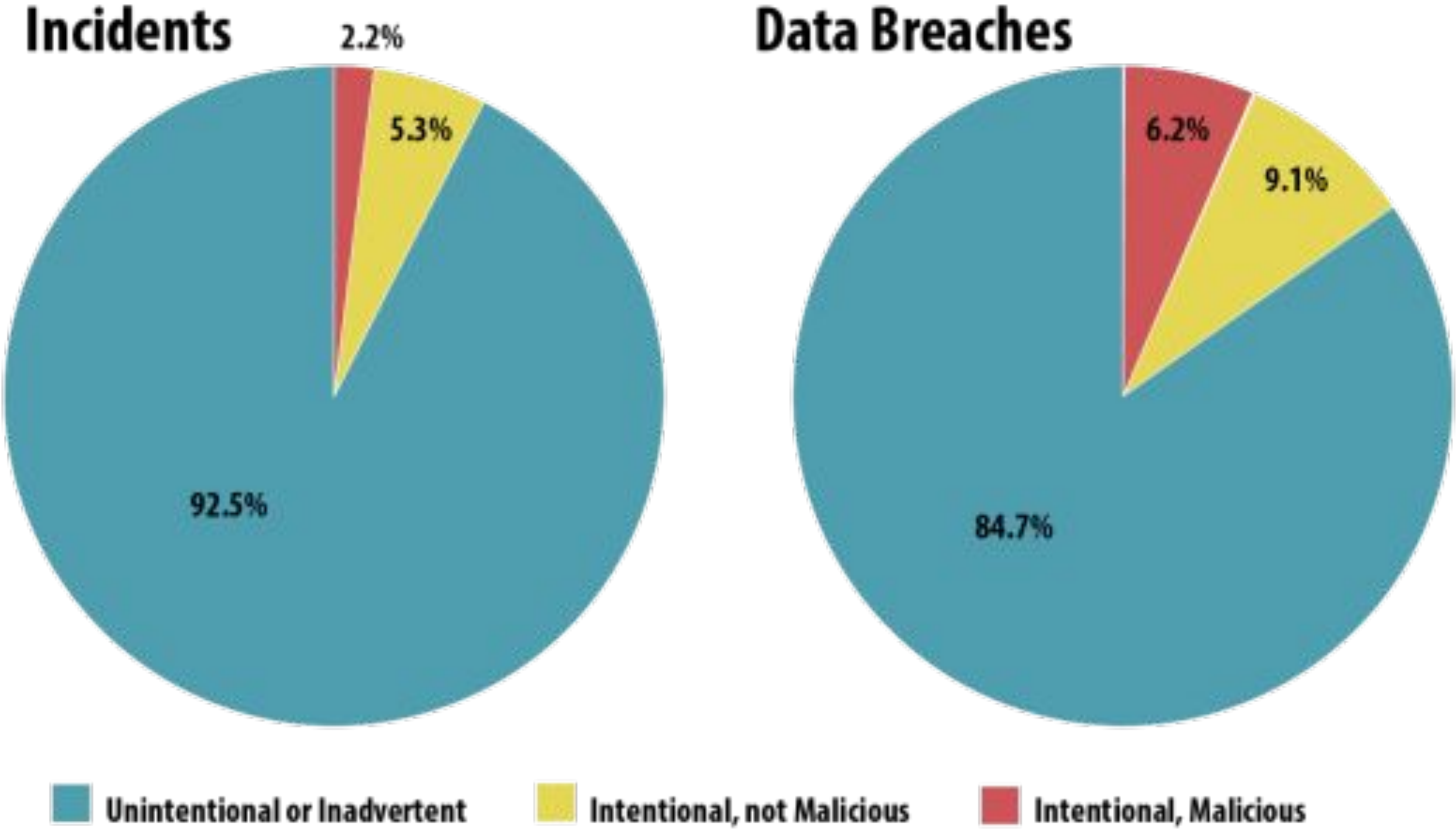
- Security Policy
- Social Engineering
- High Value Targets
- Authentication
- Default Credentials
- Default Settings
- Access Management
- Operational Security
- Updates
- Backups

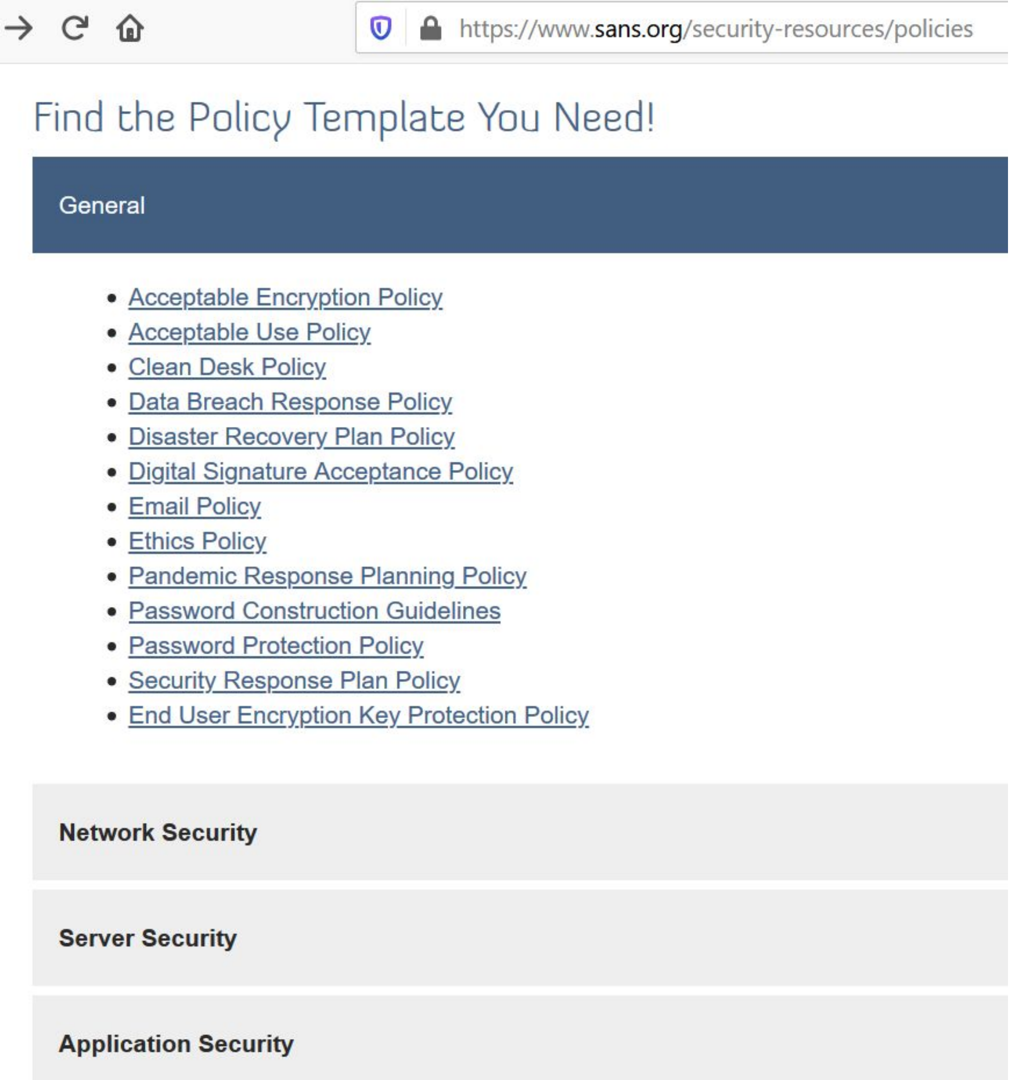
Security Policy

2018 V. 2017 DATA BREACHES BY INDUSTRY



Nature of an incident or breach





https://www.sans.org/security-resources/policies

Find the Policy Template You Need!

General

- Acceptable Encryption Policy
- Acceptable Use Policy
- Clean Desk Policy
- Data Breach Response Policy
- Disaster Recovery Plan Policy
- Digital Signature Acceptance Policy
- Email Policy
- Ethics Policy
- Pandemic Response Planning Policy
- Password Construction Guidelines
- Password Protection Policy
- Security Response Plan Policy
- End User Encryption Key Protection Policy

Network Security

Server Security

Application Security

Security Policy Exercise

1. Find out if your organization has a security policy.
2. Read the entire policy and take notes.
3. If you have an IT department, ask them about anything you think is missing from the policy.
4. If you're a small organization, look at the SANS templates and create or update the security policy (sans.org/security-resources/policies).

Social Engineering

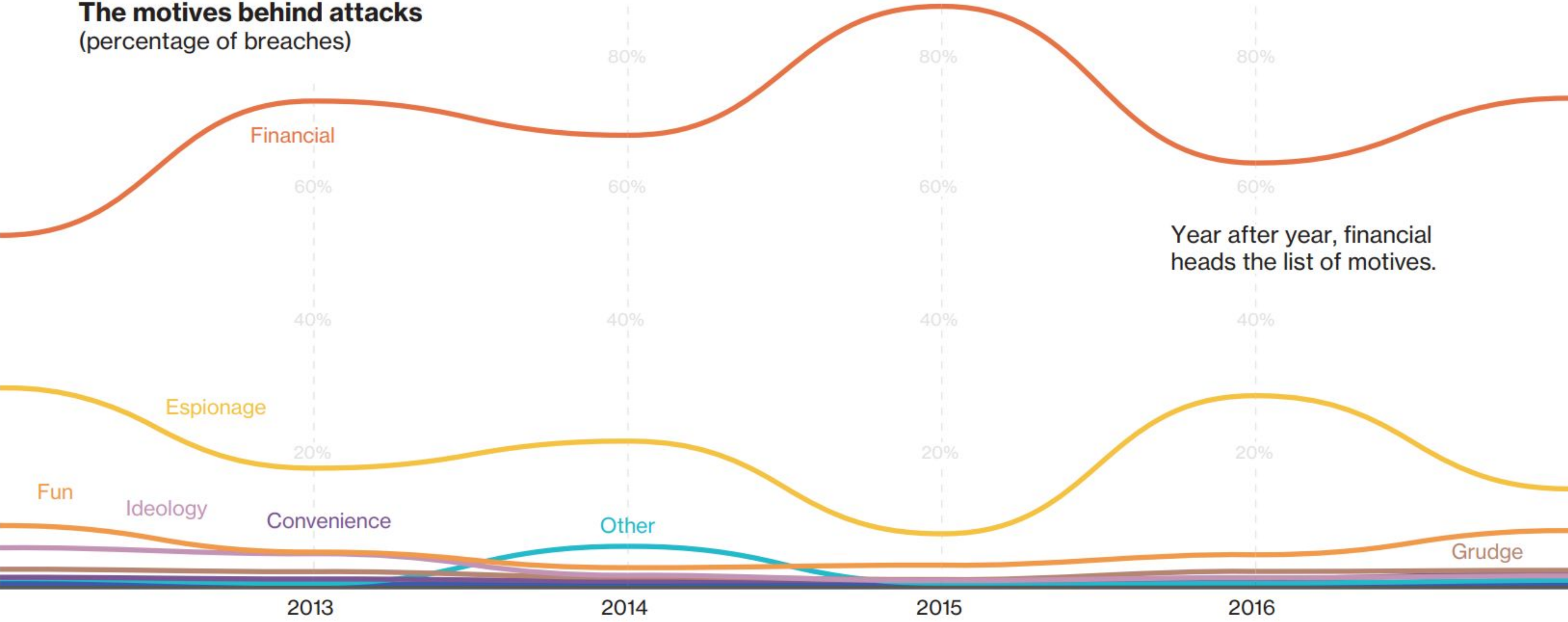
Phishing plays a role in

32% of all breaches

78% of cyber-espionage incidents*

The motives behind attacks

(percentage of breaches)



Year after year, financial heads the list of motives.

48%

of malicious email attachments are Office files—up from just 5 percent in 2017

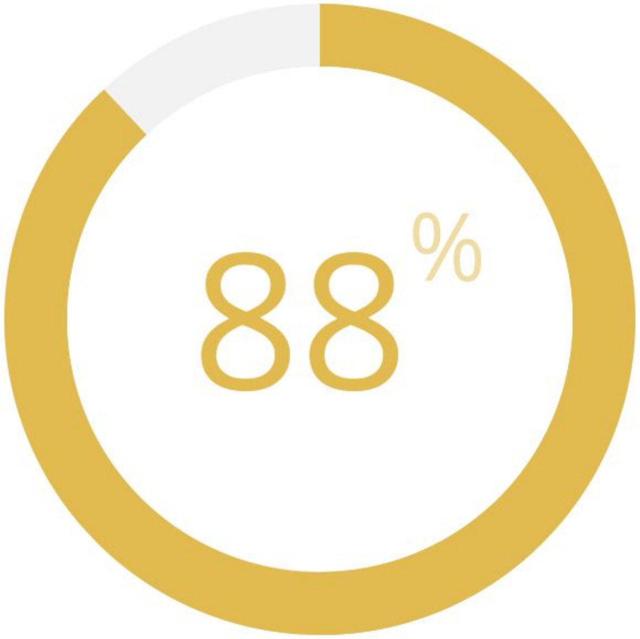
Social Engineering Exercise

1. The next time you’re at an airport or bar, eavesdrop on conversations.
2. Try to learn about a person’s:
   a. Employer
   b. Job
   c. City
   d. School
   e. Family
3. Look for that person on LinkedIn, Facebook, Twitter, etc. and see what information could be used for a social engineering attack

High Value Targets

Saw Email-Based Spoofing of Business Partners or Vendors

It doesn’t take more than a cleverly spoofed email or a damaging text message to trick even the most skilled team member.



High Value Target Exercise

1. Identify the employee and client high value targets in your organization.
2. List all the fraud or hacking attacks against these targets you can think of.
3. Identify any procedures or processes in place to prevent these attacks.
4. Consider strategies to prevent these attacks and implement them.

Authentication

#1 REASON

Why Credential Stuffing Attacks Work

Recycled Passwords

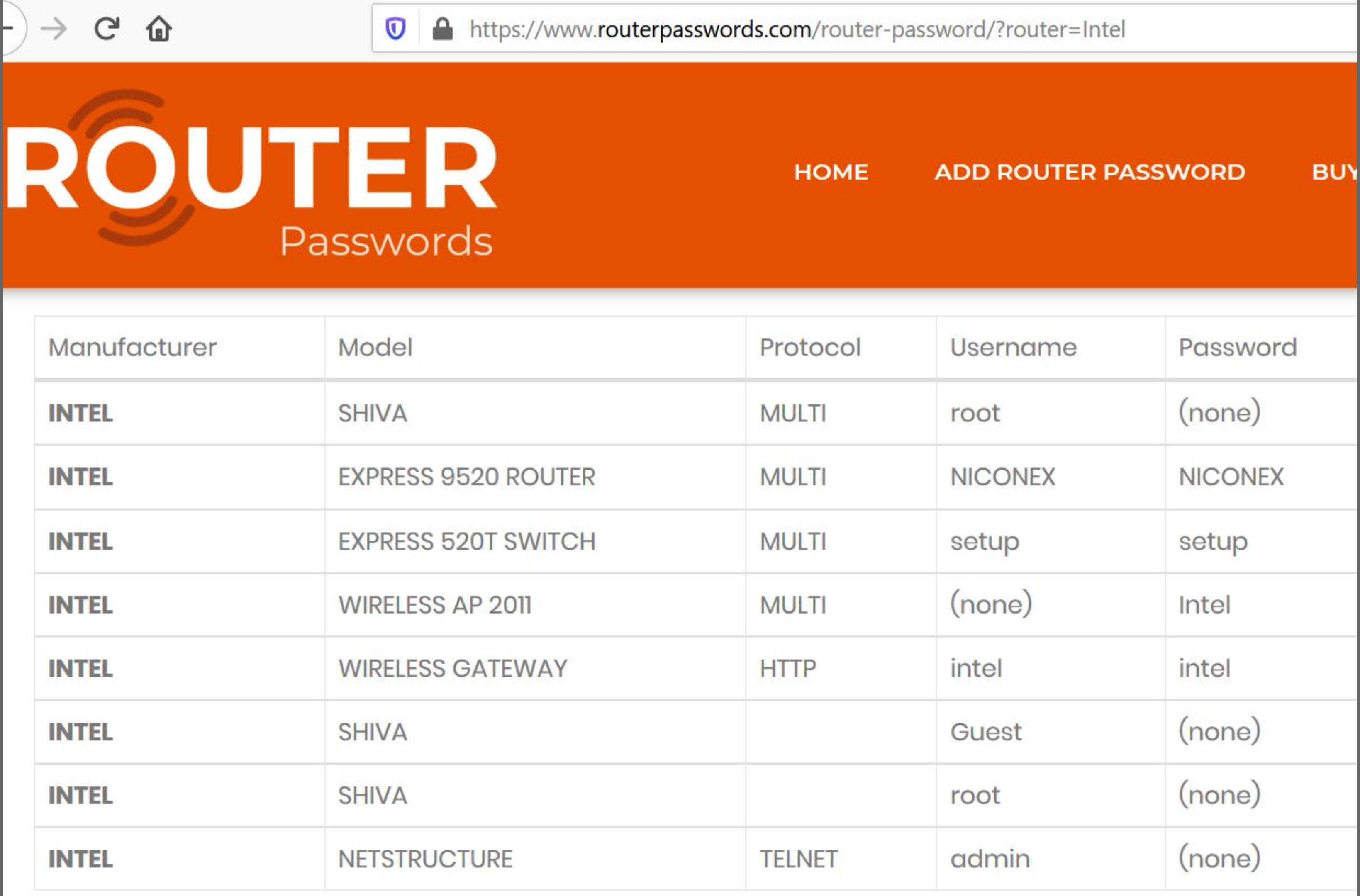
Why Accounts Are Targeted

Same email address or username discovered in multiple breaches

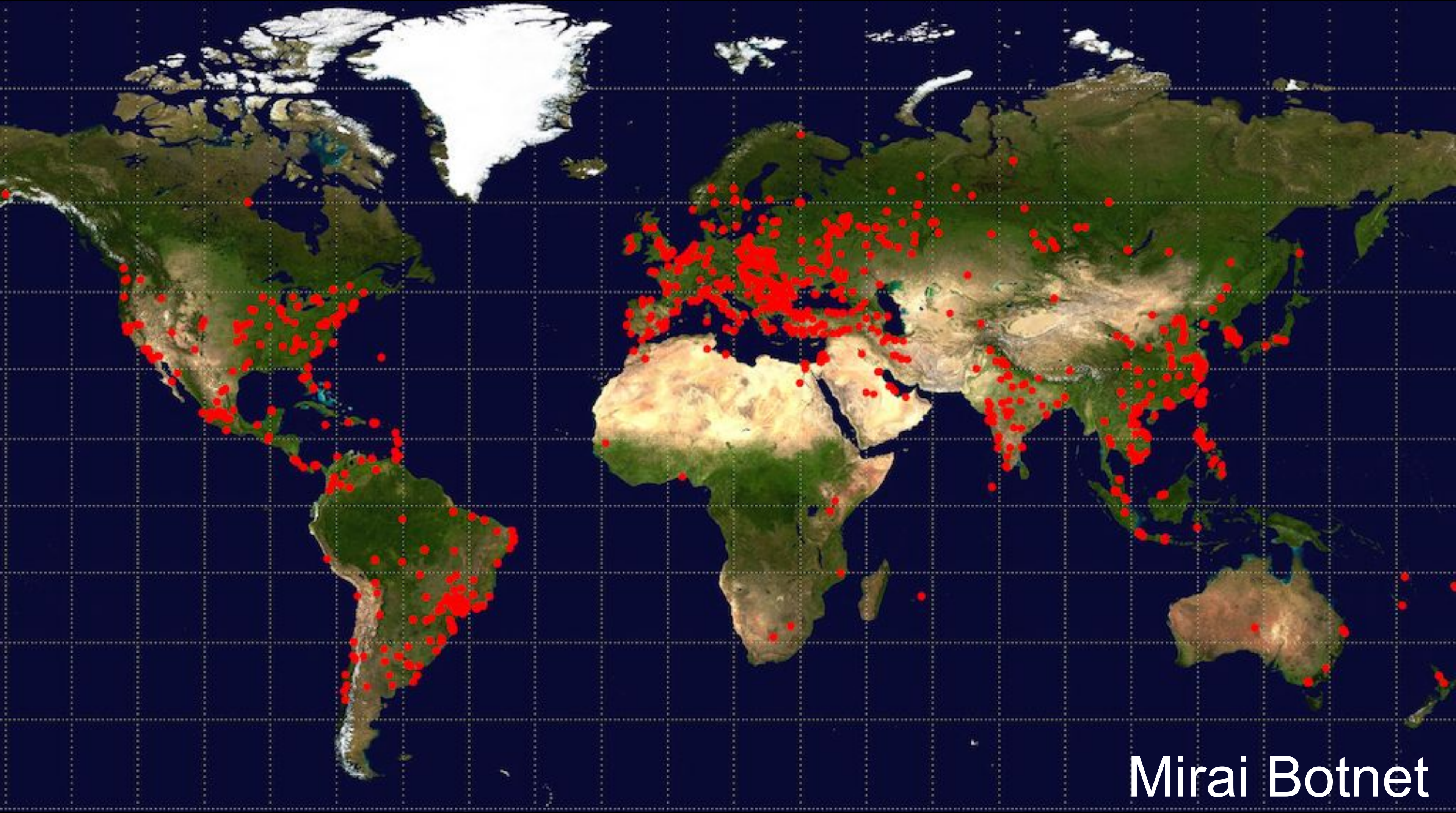
Authentication Exercise

1. Install a password manager like 1password.
2. Search haveibeenpwned.com for your home and work email address.
3. Change any compromised passwords wherever they were used.
4. Change passwords and security questions to every site with an account.
5. Add MFA like Authy or Google Authenticator where available, or use an SMS or email option if it’s all that is offered.
6. BONUS: Upgrade to a team password manager and do this exercise for your entire family.

Default Credentials


https://www.routerpasswords.com/router-password/?router=Intel
ROUTER
Passwords
HOME
ADD ROUTER PASSWORD
BUY

Manufacturer	Model	Protocol	Username	Password
INTEL	SHIVA	MULTI	root	(none)
INTEL	EXPRESS 9520 ROUTER	MULTI	NICONEX	NICONEX
INTEL	EXPRESS 520T SWITCH	MULTI	setup	setup
INTEL	WIRELESS AP 2011	MULTI	(none)	Intel
INTEL	WIRELESS GATEWAY	HTTP	intel	intel
INTEL	SHIVA		Guest	(none)
INTEL	SHIVA		root	(none)
INTEL	NETSTRUCTURE	TELNET	admin	(none)

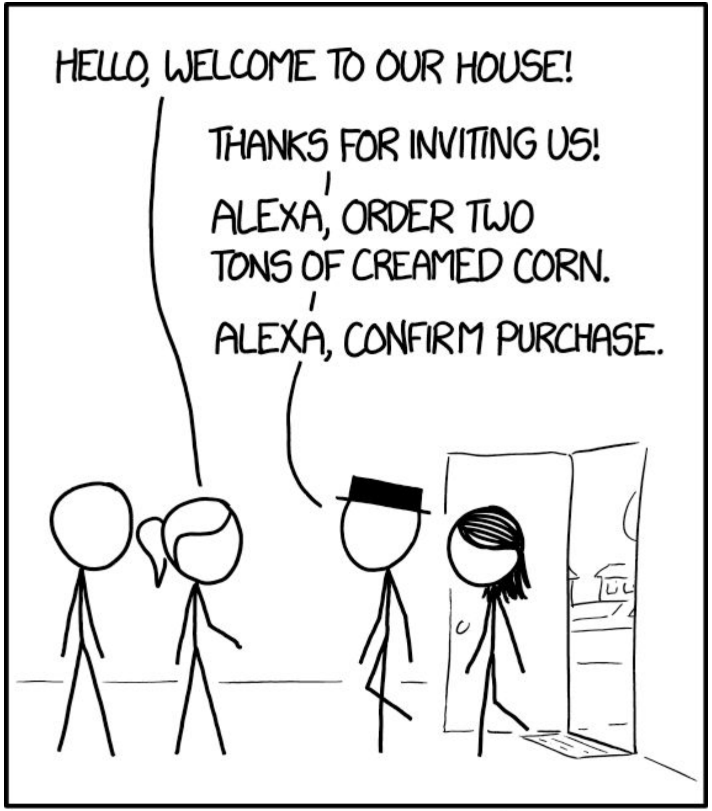


Mirai Botnet

Default Credentials Exercise

1. At home, change:
    a. Default router and wifi password
    b. Default computer password on any laptops or desktops
    c. Default passwords on all wifi devices (i.e., printers and cameras)
    d. BONUS: use IoTSeeker to find default passwords on IoT devices (information.rapid7.com/iotseeker.html)
2. At work, check that there are no default credentials on:
    a. Network devices: routers, access points, switches, firewalls, etc.
    b. Databases, web applications, and administrative interfaces
    c. BONUS: use Metasploit to scan for any default credentials

Default Settings


HELLO, WELCOME TO OUR HOUSE!
THANKS FOR INVITING US!
ALEXA, ORDER TWO TONS OF CREAMED CORN.
ALEXA, CONFIRM PURCHASE.

WHEN VISITING A NEW HOUSE, IT'S GOOD TO CHECK WHETHER THEY HAVE AN ALWAYS-ON DEVICE TRANSMITTING YOUR CONVERSATIONS SOMEWHERE.

Default Settings Exercise

1. At home, change:
    a. Default network name (SSID)
    b. Change wifi to WPA2 or WPA mode (not WEP)
    c. Change wifi encryption to AES (not TKIP or AES + TKIP)
    d. Disable WPS and UPnP features
    e. Enable the router firewall
2. Check the settings and permissions for five online accounts or mobile apps

Access Management

21% OF ALL FOLDERS

in a company were open to every employee

41% OF COMPANIES

have over 1,000 sensitive files open to every employee

88% OF COMPANIES

with over 1 million folders have over 100,000 folders open to everyone

34% OF USER ACCOUNTS

are stale but enabled

65% OF COMPANIES

have over 1,000 stale user accounts

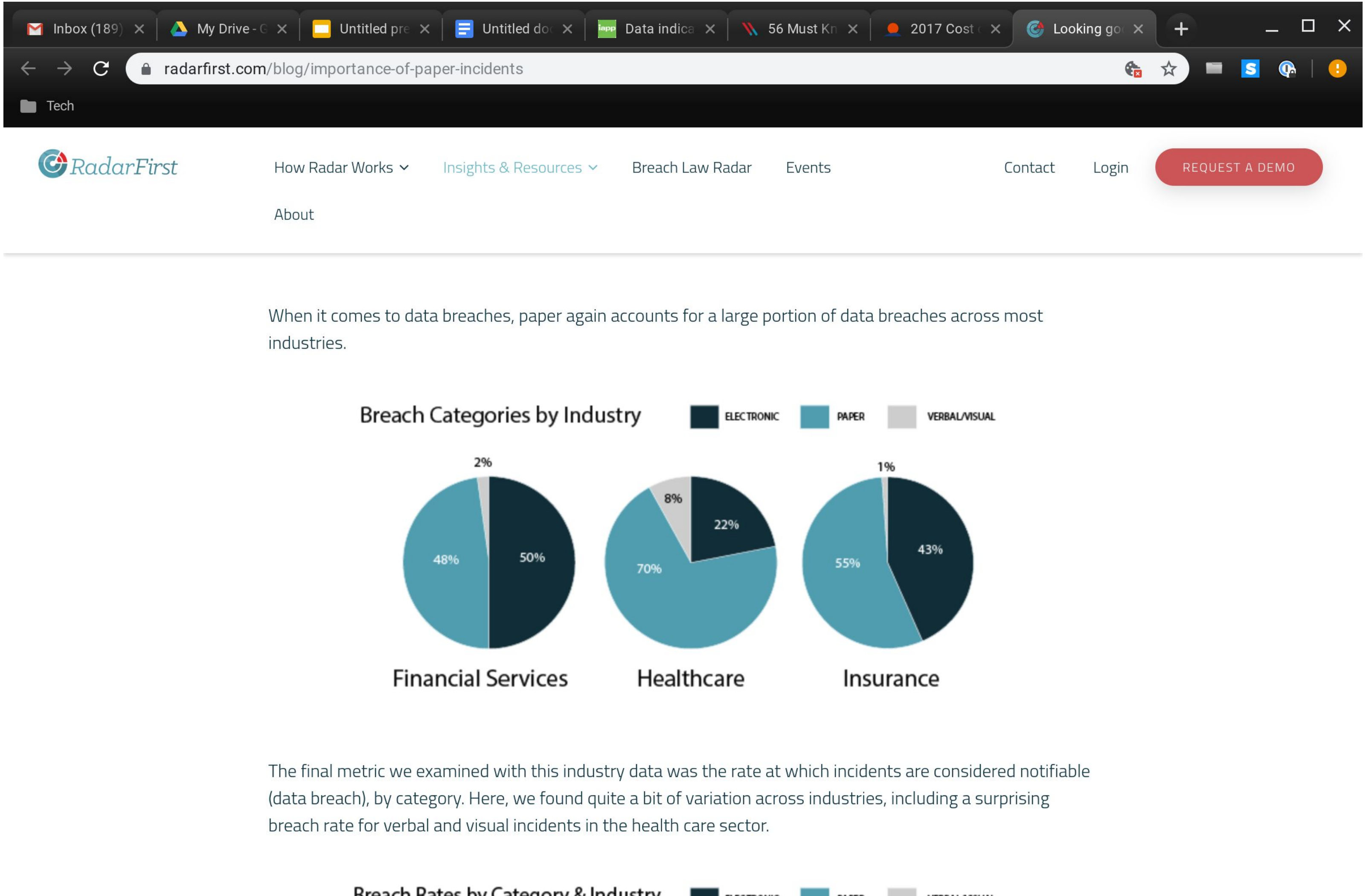
64% OF USER ACCOUNTS

are stale or inactive

Access Management Exercise

1. At home, change:

Operational Security (OpSec)



When it comes to data breaches, paper again accounts for a large portion of data breaches across most industries.

Breach Categories by Industry

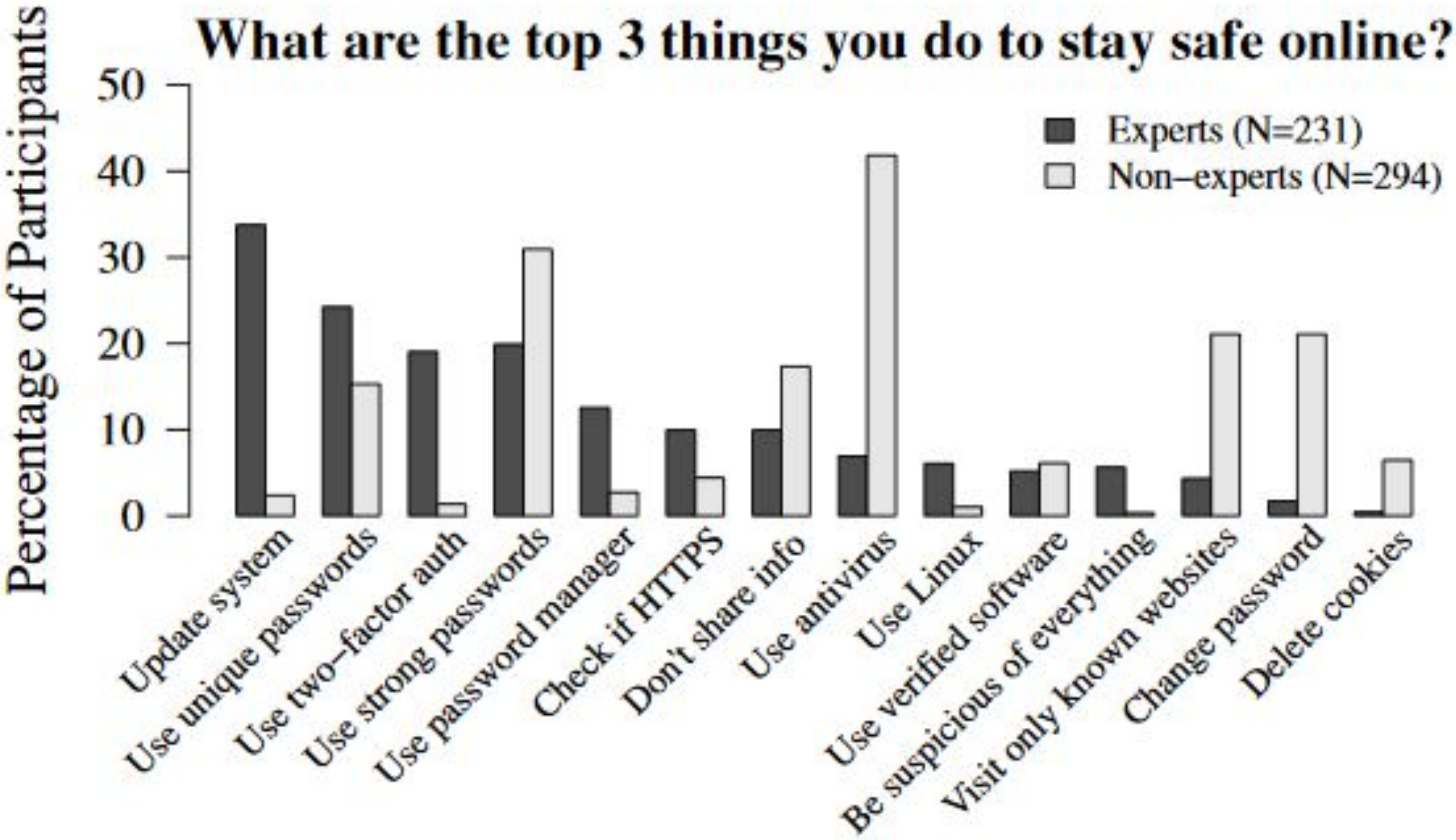
The final metric we examined with this industry data was the rate at which incidents are considered notifiable (data breach), by category. Here, we found quite a bit of variation across industries, including a surprising breach rate for verbal and visual incidents in the health care sector.

Breach Rates by Category & Industry

OpSec Exercise

1. At home, change:

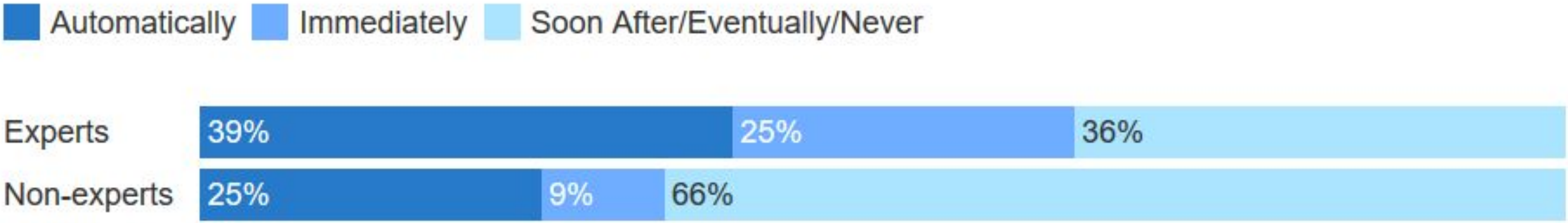
Updates



What are the top 3 things you do to stay safe online?
Percentage of Participants
50
40
30
20
10
0
■ Experts (N=231)
□ Non–experts (N=294)
Update system
Use unique passwords
Use two–factor auth
Use strong passwords
Use password manager
Check if HTTPS
Don't share info
Use antivirus
Use Linux
Use verified software
Be suspicious of everything
Visit only known websites
Change password
Delete cookies

How soon do you install updates?

Many experts install software updates fairly quickly, but nearly one-third are relatively slow, and two-thirds of non-experts are also slow at updating.



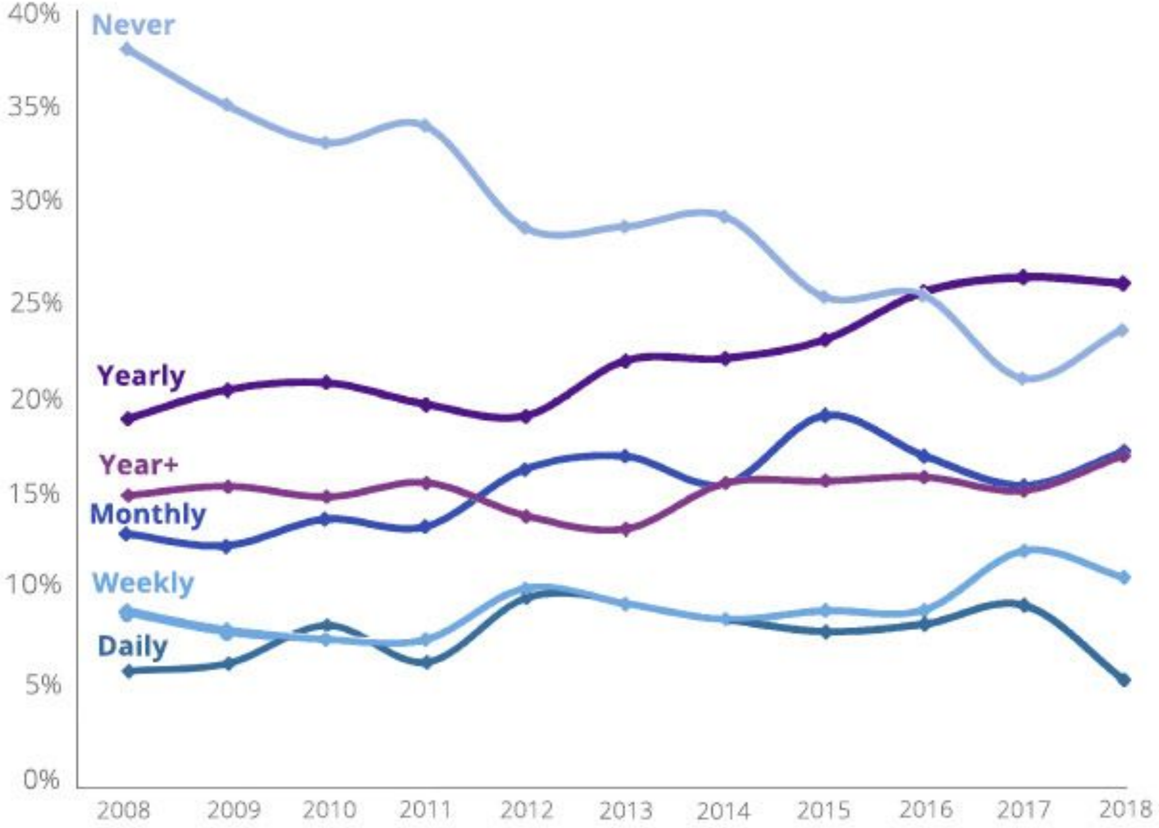
Update Exercise

1. At home, change:

Backups

Computer Backup Frequency

When asked: "how often do you backup all the data on your computer?"



Backup Exercise

1. At home, change:

Questions?

References

1. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-phishing-baiting-the-hook-infographic-2019.pdf
2. https://www.mimecast.com/the-state-of-email-security-2019/
3. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf
4. https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf
5. https://www.varonis.com/2018-data-risk-report/
6. https://interactive.symantec.com/istr24-web
7. https://www.radarfirst.com/blog/importance-of-paper-incidents
8. https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/
9. https://umbrella.cisco.com/blog/2017/01/05/future-assaulting-internet-mirai/
10. https://xkcd.com/1807/
11. https://www.sans.org/security-resources/policies/
12. https://www.backblaze.com/blog/computer-backup-awareness-in-2018/
13. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf
14. https://theconversation.com/the-petya-ransomware-attack-shows-how-many-people-still-dont-install-software-updates-77667