# Cybersecurity Basics

## The Fundamentals of Protecting Sensitive Data in Health & Human Services

October 2024

**CaseWorthy**™

# Presenter



Chief Information Security Officer

**Shayne Champion**

# Agenda

**01** Hackers

**02** Cybersecurity Basics

**03** Q&A

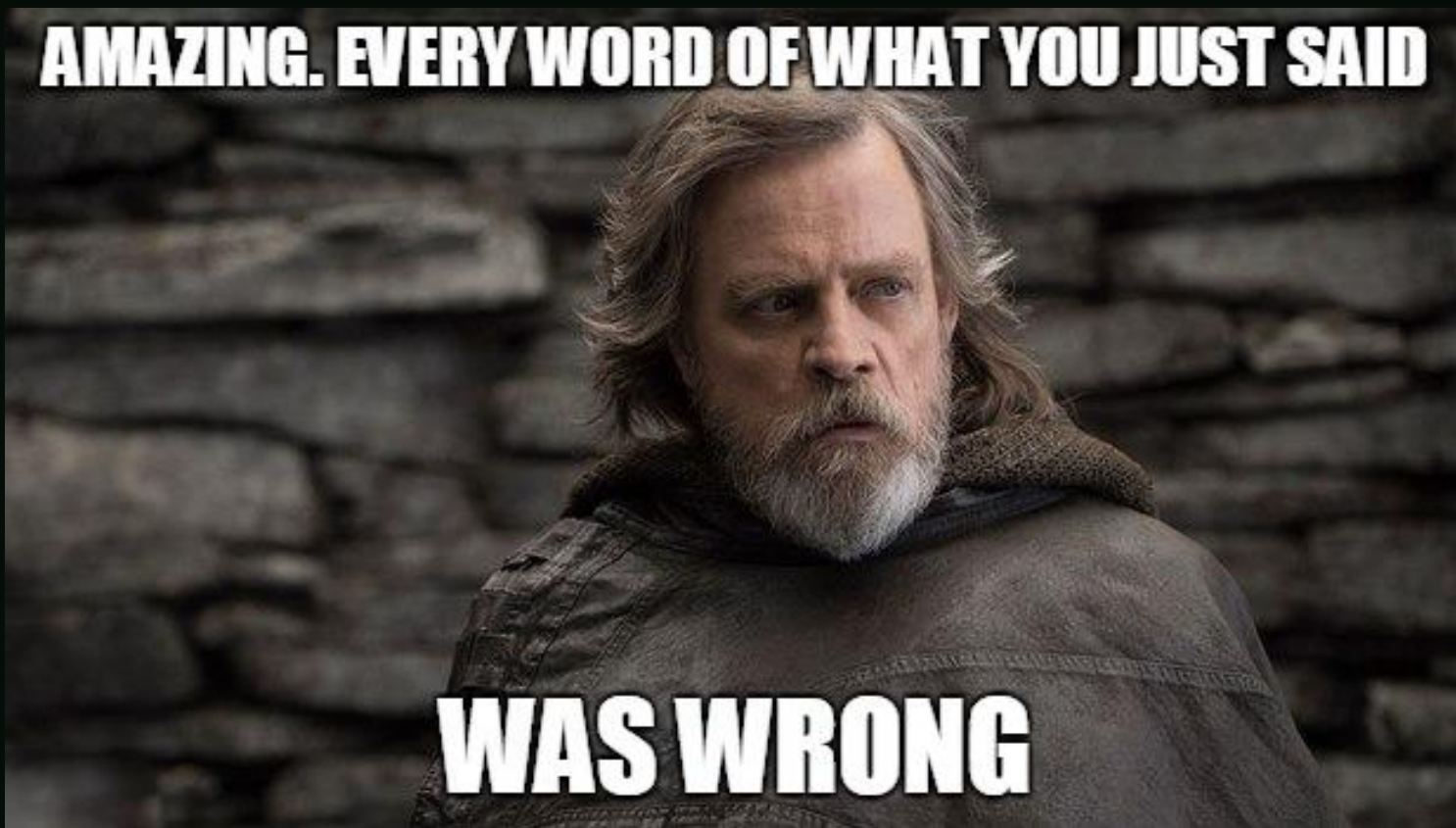# Hackers

# What is a Hacker?

# What is a Hacker?





Levy, S. (2010). *Hackers: Heroes of the Computer Revolution.*
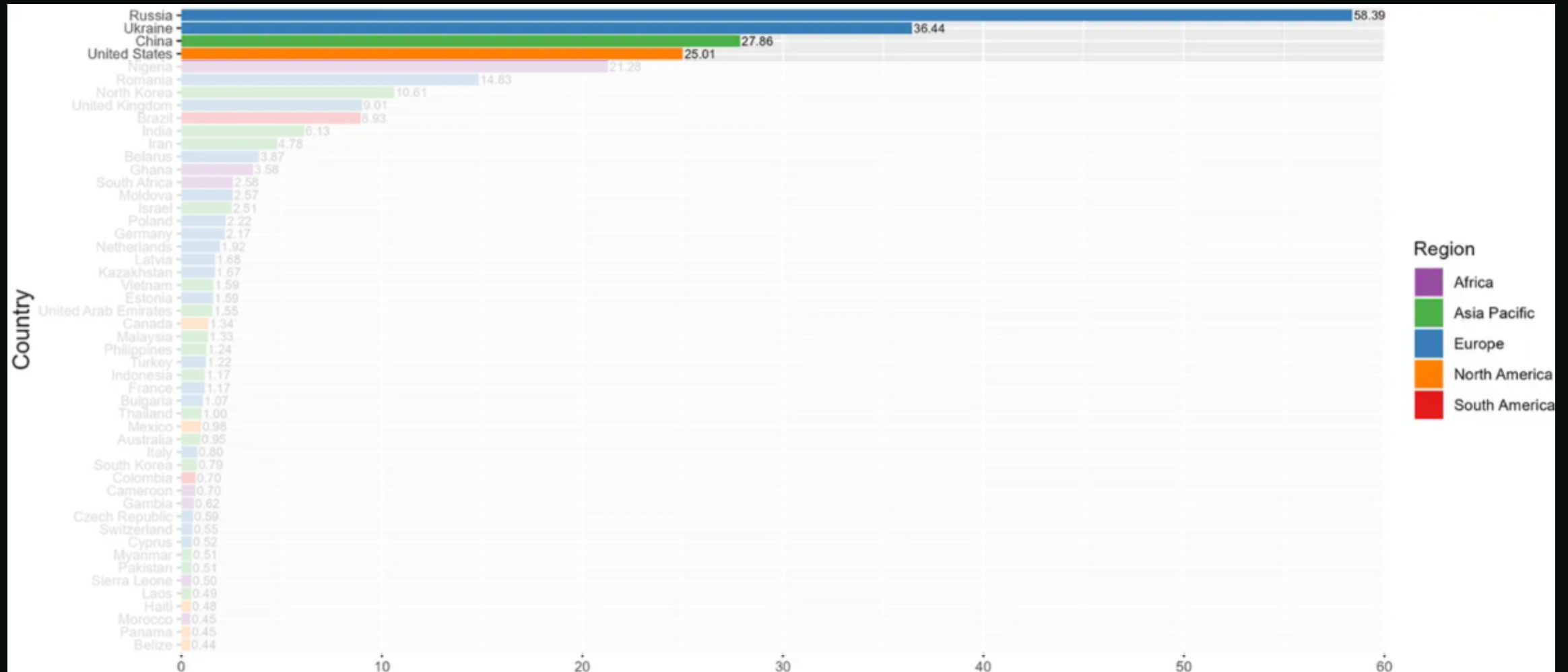
# What's a Hacker Look Like?



Pen Tester

Kevin Mitnick

Me

Mitnick, K., Simon, W. (2011). *Ghost in the Wires*.
https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev
https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

# Where the Hackers Live

# Where the Hackers Live



**1** (58.39)

Smash & Grab

https://cyberdefensereview.army.mil/Portals/6/Documents/2024_Spring/Jackson_CDRV9N1-Spring-2024.pdf

Krebs, B. (2014). *Spam Nation*.

# Where the Hackers Live



**2**
(36.44)

**Intelligence & Support**

https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-is-on-the-front-lines-of-global-cyber-security/
https://therecord.media/ukraine-cyberattacks-aiding-ground-war-russia
https://www.brookings.edu/articles/russia-ukraine-and-organized-crime-and-illicit-economies-in-2024/

# Where the Hackers Live



**3** (27.86)

**Insider Threat**

Zetter, K. (2021) *Countdown to Zero Day*.
https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

# Where the Hackers Live


**Su Bin**

**J-31 (China)**

**F-35 (USA)**

**3** (27.86)

**Insider Threat**

## F-35 "Lightning II" Stealth Fighter

- **$1.5 Trillion** program
- **14 years to develop**
  - Development started 1992
  - First flight: Dec 2006

- China steals blueprints in **2011**
  First flight: **Oct 2012**

Zetter, K. (2021) *Countdown to Zero Day*.
https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china
https://www.sandboxx.us/news/the-man-who-stole-americas-stealth-fighters-for-china/
https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months

# Where the Hackers Live



**4** (25.01)

## Hi Tech, Crusaders, & Careless

https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating
https://cyberscoop.com/potent-youth-cybercrime-ring-made-up-of-1000-people-fbi-official-says

# How Much Do Hackers Make?

## 10.37 connected devices per person[4]

According to the FBI, US cybercrime losses alone exceeded **$12.5 Billion** in 2023.[1]

Global Impact of Cyber Crime[2]
- **$8 trillion** per Year
- **$667 billion** per Month
- **$154 billion** per Week
- **$21.9 billion** per Day
- **$913 million** per Hour
- **$15.2 million** per Minute
- **$255,000** per Second

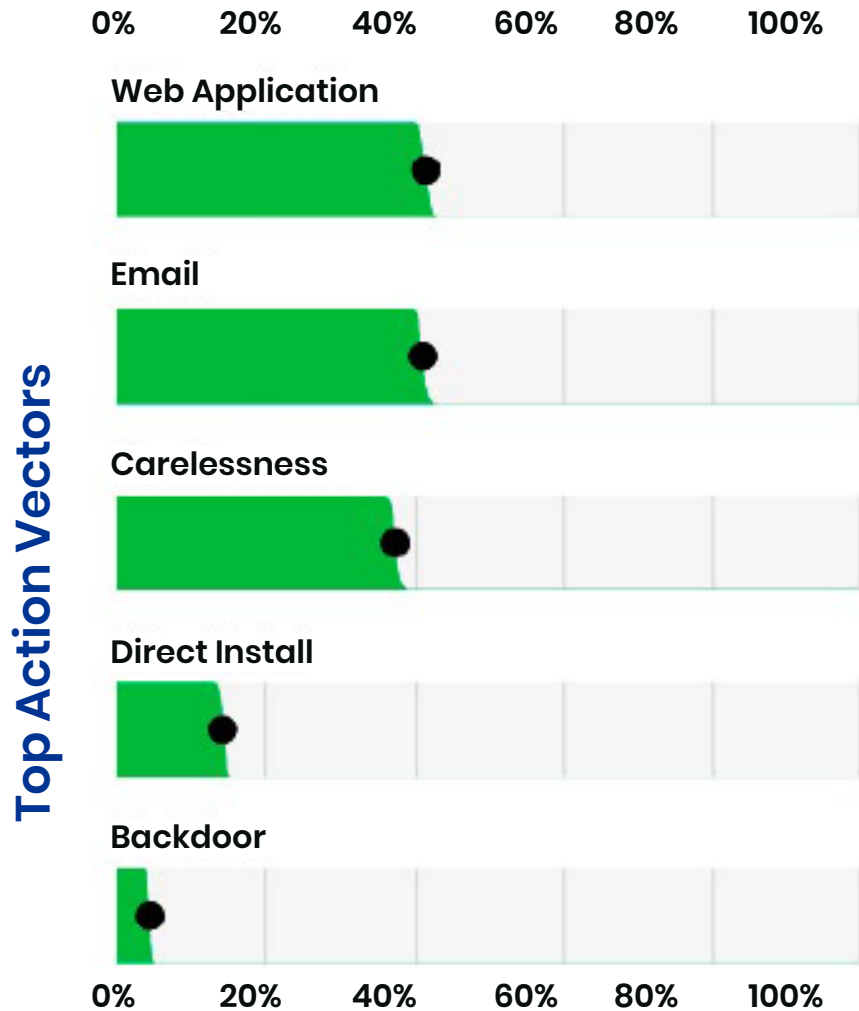Global cybercrime collectively represents the **world's third-largest economy by GDP**, only trailing the US and China[3]
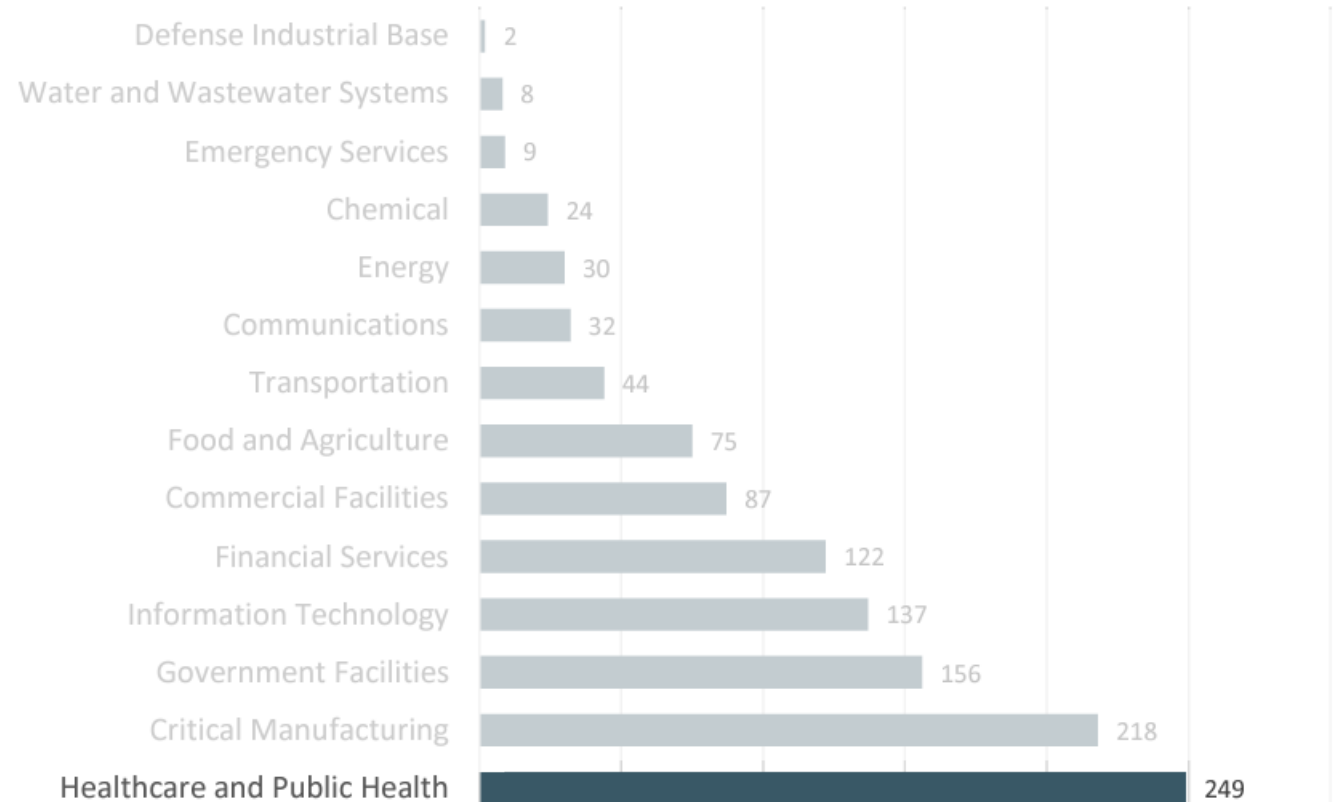
Sources:
1. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
2. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
3. https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/
4. https://www.statista.com/statistics/1107206/average-number-of-connected-devices-us-house/

# What Attacks Are Hackers Using?

**Top Action Vectors**

0%  20%  40%  60%  80%  100%

**Web Application**

**Email**

**Carelessness**

**Direct Install**

**Backdoor**

0%  20%  40%  60%  80%  100%

## Infrastructure Sectors Affected by Ransomware

| Sector | Value |
|---|---|
| Defense Industrial Base | 2 |
| Water and Wastewater Systems | 8 |
| Emergency Services | 9 |
| Chemical | 24 |
| Energy | 30 |
| Communications | 32 |
| Transportation | 44 |
| Food and Agriculture | 75 |
| Commercial Facilities | 87 |
| Financial Services | 122 |
| Information Technology | 137 |
| Government Facilities | 156 |
| Critical Manufacturing | 218 |
| Healthcare and Public Health | 249 |

# What Do Hackers Want From YOU?

# 2024 DBIR

# 2024 DBIR

https://www.verizon.com/business/resources/reports/dbir/
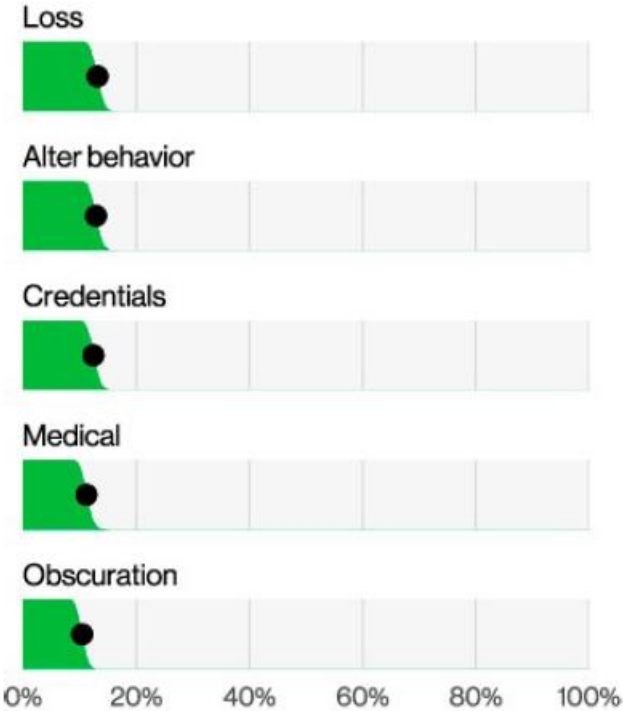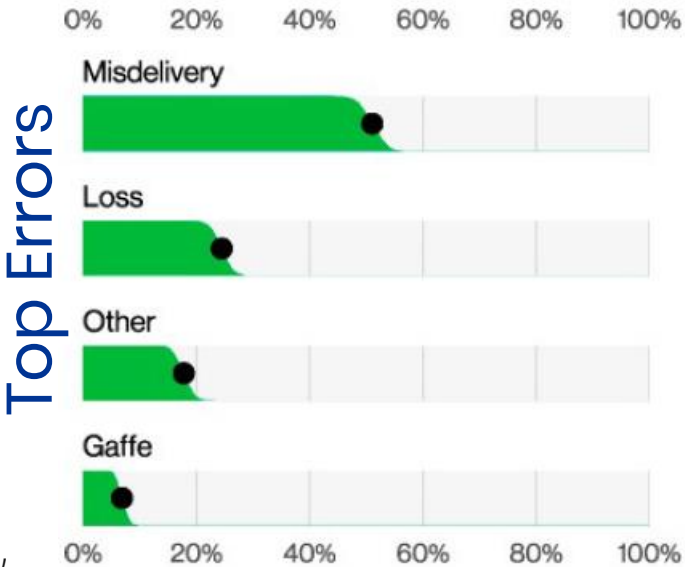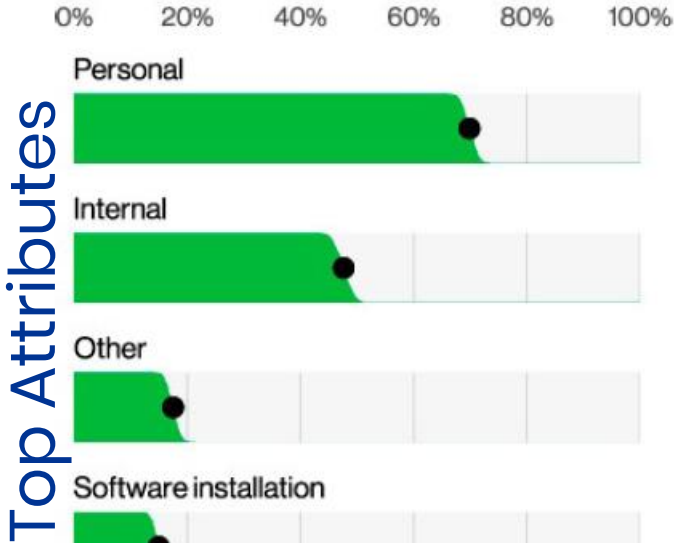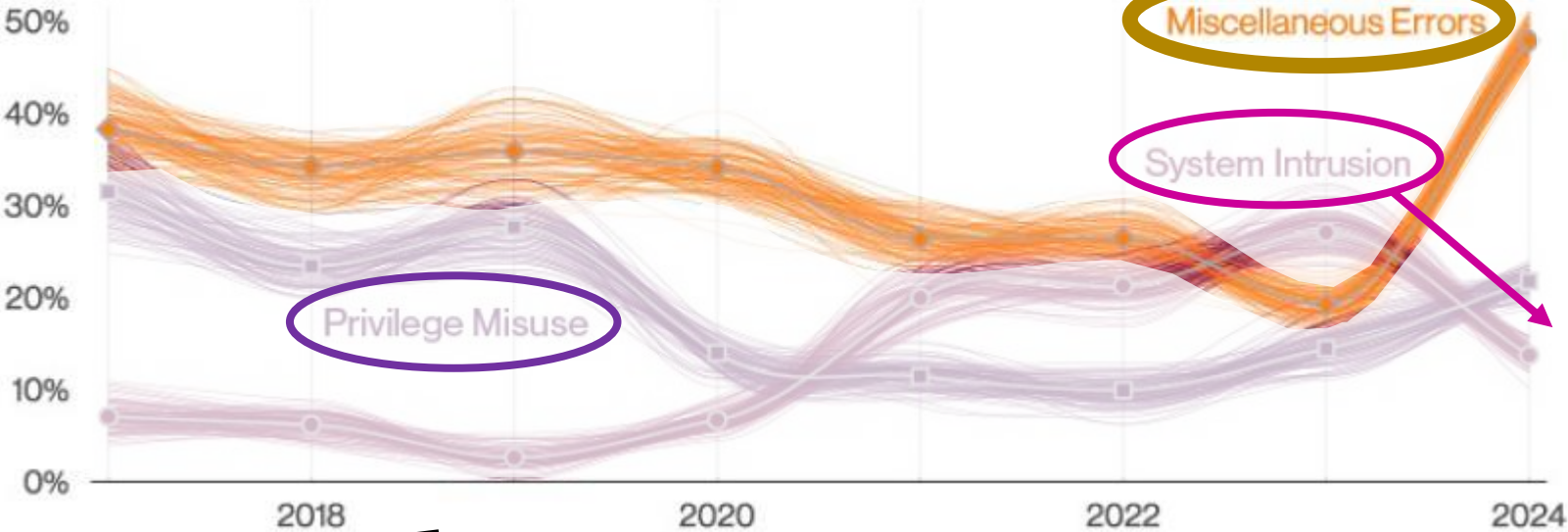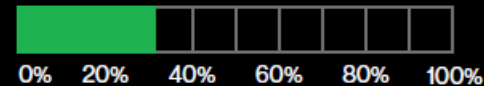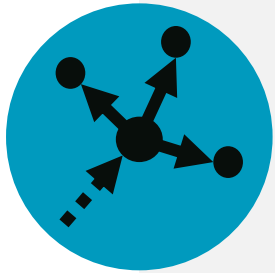
# Why Your Personal Information?



Stolen credentials remain massively popular.

31% of all breaches over the past 10 years have involved the Use of stolen credentials.

31%

0%  20%  40%  60%  80%  100%

# Why Your Personal Information?

## Pivoting

- Leads to your email accounts
- Friends & professional acquaintances
- Password reuse

https://techreport.com/statistics/cybersecurity/password-reuse-statistics/

## Tailored Attacks

- Learn what you like, what you do, and where you go
- Phishing
- Artificial Intelligence

https://www.sangfor.com/blog/cybersecurity/defining-ai-hacking-rise-ai-cyber-attacks/
https://ir.zscaler.com/news-releases/news-release-details/zscaler-research-finds-60-increase-ai-driven-phishing-attacks

## Financial Information

- Getting your bank accounts
- Profits & income sources

https://ipdefenseforum.com/2024/03/u-n-report-north-korea-financing-weapons-program-with-cybercrime/

## Disguise

- Using your identity online
- Using your identity to enter the country
- Focus on the elderly, deceased, and disabled

https://www.neighborsfcu.org/fraud-latest-scams-targeting-people-with-disabilites/

# Protecting Everybody

**CaseWorthy's products contain data for over 2.95 million people**

# About Nathan

Nathan Chandler lives in an adult group home with 4 other individuals. While he has a supportive family, his mother is elderly, and he has no other family. Nathan works at Walmart as a greeter. He wants to become more involved in the community and is volunteering at an animal shelter to expand his social circle.

Eventually he would like to have a girlfriend and has recently joined Match.com. Nathan would also like to move out of his group home and is learning how to prepare his own meals without support from the staff. Nathan is partially deaf, has moderate intellectual disabilities, and impaired motor skills. As such he needs a strobe light and bed shaker in case of an emergency evacuation.



## Nathan Harris

Age: 28
Location: Portland, OR

The **only** people who should have access to Nathan's records are **Nathan** and **those who he has authorized**.

Authorized users should **only** have access to the specific types of data Nathan approved.

# CYBERSECURITY BASICS

## What YOU Can Do To Stop Them

- Web Applications
- Email
- Carelessness
- Ransomware

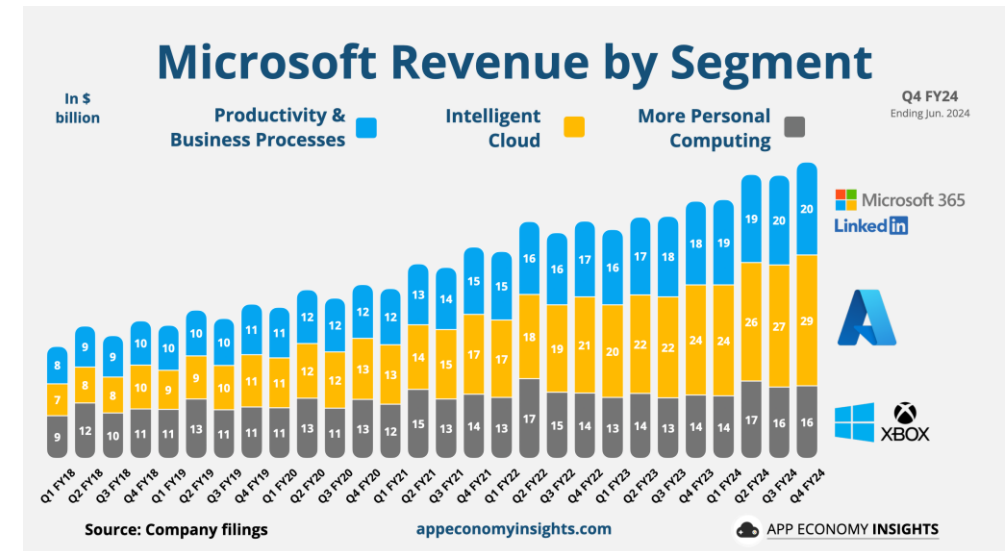# Web Applications

# Expansion of Cloud Computing

## Amazon Web Services (AWS)



**Amazon Quarterly Results (in millions)**

Legend: Revenue (Net Sales) · Profit (Net Income)

Source: Amazon Quarterly and Annual Reports

GEEKWIRE

## Microsoft Azure



**Microsoft Revenue by Segment**

In $ billion

Productivity & Business Processes · Intelligent Cloud · More Personal Computing

Q4 FY24 Ending Jun. 2024

Microsoft 365 · LinkedIn · XBOX

Source: Company filings

appeconomyinsights.com

APP ECONOMY INSIGHTS

# Web Application Security

## Developers

- **OWASP Top 10**
  https://owasp.org/www-project-top-ten/

- **Encryption**

- **Web Application Firewalls (WAF)**

# Web Application Security

## Developers

- **OWASP Top 10**
  https://owasp.org/www-project-top-ten/

- **Encryption**

- **Web Application Firewalls**

## Everybody

- **Secure Links**

# Web Application Security


Choose your third parties wisely.

15%
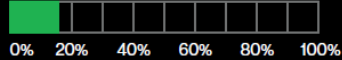
15% of breaches involved a third party—including data custodians or hosting partner infrastructures being breached, and direct or indirect software supply chain issues.

0%  20%  40%  60%  80%  100%


SEEMS A LITTLE CRAZY
...until it isn't crazy!

## Everybody
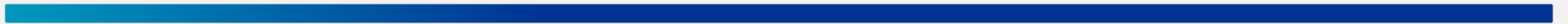
- **Secure Links**

- **Mobile Devices**
  Microsoft Intune

- **Due Diligence**

- **Skepticism**


See something.
Say something.

Email

# Phishing

- **Watch for Red Flags:**
  - Suspicious URLs
  - Generic titles
  - Using pressure to force you
  - Bad spelling or grammar
  - Unexpected attachments
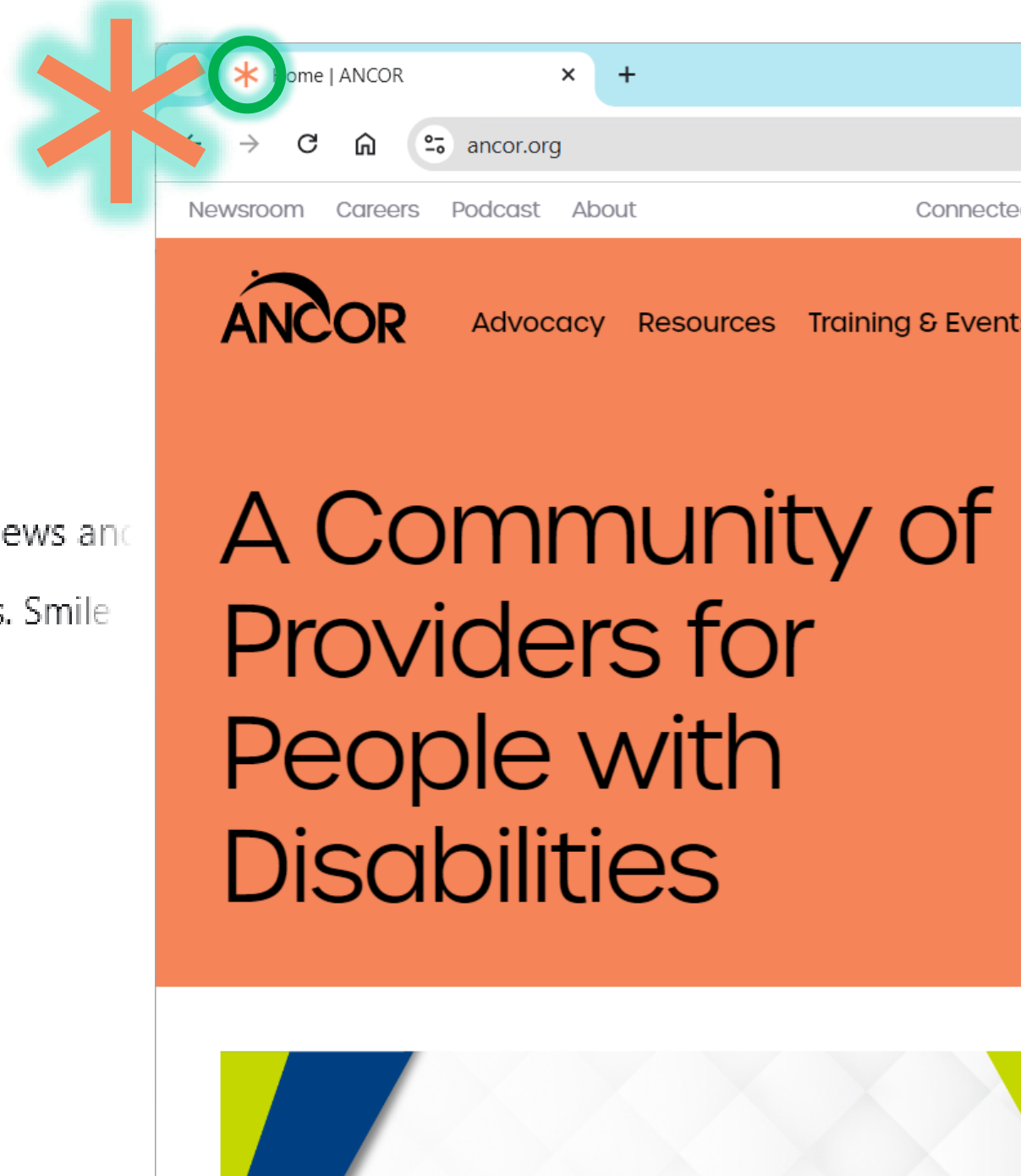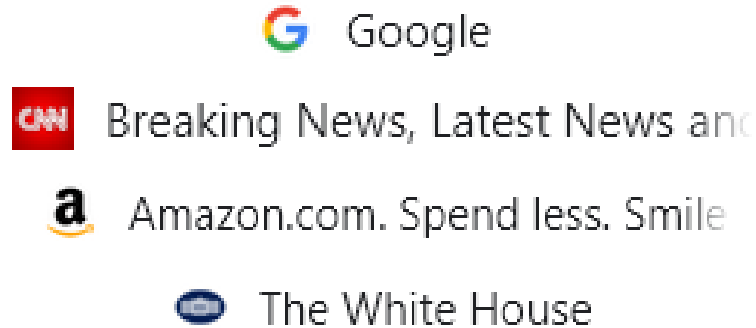
- **Favicons**

# Phishing

- **Watch for Red Flags:**
  - Suspicious URLs
  - Generic titles
  - Using pressure to force you
  - Bad spelling or grammar
  - Unexpected attachments

- **Favicons**

- **Phishing Training**



## Falling for Phishing—fast

**< 60** sec.

The median time for users to fall for phishing emails is less than 60 seconds.

# Email Authentication

**SPF**
**(Sender Policy Framework)**

**DKIM**
**(DomainKeys Identified Mail)**

**DMARC**
**(Domain-based Message Authentication, Reporting, and Conformance)**

https://www.mimecast.com/content/dkim-spf-dmarc-explained/
https://mxtoolbox.com/dmarc/dmarc-email-tools

# Carelessness

## Software Updates

- Implement patch automation

- Identify and cover all devices

- Test and roll out patches carefully

**Vulnerabilities are showing.**

## 180%

0%      100%      200%

Exploitation of vulnerabilities as an initial access step for a breach grew by 180%— almost triple that of last year— fueled in part by the MOVEit vulnerability and several other zero-day exploits used by ransomware actors.

https://www.techtarget.com/searchenterprisedesktop/tip/12-best-patch-management-software-and-tools

# Carelessness

## Software Updates

- Implement patch automation
- Identify and cover all devices
- Test and roll out patches carefully

## Passwords & MFA

- Passwords vs Passphrases
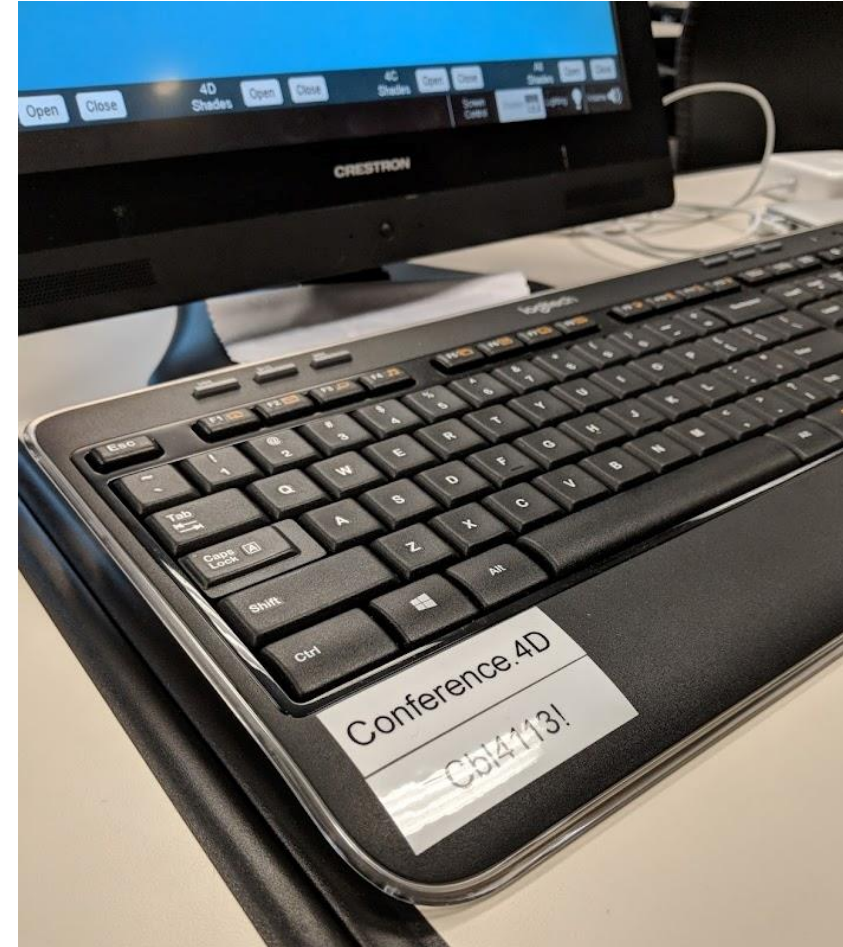
# Password (In)Security

| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|---|---|---|---|---|---|
| 4 | INSTANTLY | INSTANTLY | INSTANTLY | INSTANTLY | INSTANTLY |
| 5 | INSTANTLY | INSTANTLY | INSTANTLY | INSTANTLY | INSTANTLY |
| 6 | INSTANTLY | INSTANTLY | INSTANTLY | INSTANTLY | INSTANTLY |
| 7 | INSTANTLY | INSTANTLY | 2 SECS | 7 SECS | 31 SECS |
| 8 | INSTANTLY | INSTANTLY | 2 MINS | 7 MINS | 39 MINS |
| 9 | INSTANTLY | 10 SECS | 1 HOUR | 7 HOURS | 2 DAYS |
| 10 | INSTANTLY | 4 MINS | 3 DAYS | 3 WEEKS | 5 MONTHS |
| 11 | INSTANTLY | 2 HOURS | 5 MONTHS | 3 YEARS | 34 YEARS |
| 12 | 2 SECS | 2 DAYS | 24 YEARS | 200 YEARS | 3K YEARS |
| 13 | 19 SECS | 2 MONTHS | 1K YEARS | 12K YEARS | 202K YEARS |
| 14 | 3 MINS | 4 YEARS | 64K YEARS | 750K YEARS | 16M YEARS |
| 15 | 32 MINS | 100 YEARS | 3M YEARS | 46M YEARS | 1BN YEARS |
| 16 | 5 HOURS | 3K YEARS | 173M YEARS | 3BN YEARS | 92BN YEARS |
| 17 | 2 DAYS | 69K YEARS | 9BN YEARS | 179BN YEARS | 7TN YEARS |
| 18 | 3 WEEKS | 2M YEARS | 467BN YEARS | 11TN YEARS | 438TN YEARS |

'Secure' 8-character password example:

**R&2Lf^v!**

**TIME TO HACK:**
**39 Minutes**

Passphrases are easier to remember:

**The Hills Are Alive**

**TIME TO HACK:**
**11 Trillion Years**

https://www.alliancetech.com/crack-password/
https://www.darkreading.com/identity-access-management-security/nist-drops-password-complexity-mandatory-reset-rules

# Carelessness

## Software Updates

- Implement patch automation
- Identify and cover all devices
- Test and roll out patches carefully

## Passwords & MFA

- Passwords vs Passphrases
- Value of Multi-Factor Authentication (MFA)

### MFA Types

**1. KNOWLEDGE: Something You Know**

**2 POSSESSION: Something You Have**

**3 INHERENCE: Something You Are**

**4 LOCATION: Somewhere You Are**

# Carelessness

## Software Updates

- Implement patch automation
- Identify and cover all devices
- Test and roll out patches carefully

## Passwords & MFA

- Passwords vs Passphrases
- Value of Multi-Factor Authentication (MFA)

## Physical Security

- Clean Desk Policy
- Prevent Shoulder Surfing
- Just Be Careful

# Ransomware



## Infrastructure Sectors Affected by Ransomware

| Sector | Count |
|---|---|
| Defense Industrial Base | 2 |
| Water and Wastewater Systems | 8 |
| Emergency Services | 9 |
| Chemical | 24 |
| Energy | 30 |
| Communications | 32 |
| Transportation | 44 |
| Food and Agriculture | 75 |
| Commercial Facilities | 87 |
| Financial Services | 122 |
| Information Technology | 137 |
| Government Facilities | 156 |
| Critical Manufacturing | 218 |
| Healthcare and Public Health | 249 |
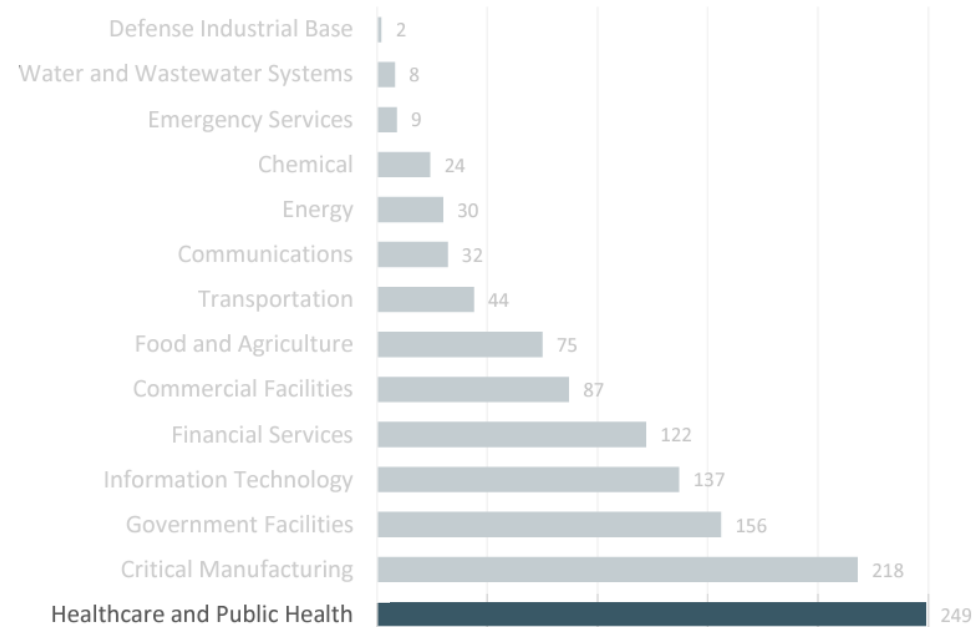
# Ransomware

## Network Segmentation

- Firewalls & DMZs
- Zero Trust Networking
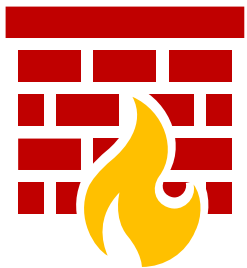
## Backups

- Offline Backups
- Inventory
- Annual Testing

## Security Fundamentals

- User Training
- Keep Devices Updated
- Password Hygiene
- Anti-Virus Software

https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf
https://www.cisa.gov/news-events/news/protecting-against-ransomware
https://www.cisa.gov/resources-tools/resources/cisa-multi-state-information-sharing-and-analysis-center-ms-isac-joint-ransomware-guide
https://cloud.google.com/beyondcorp

# Quick Review
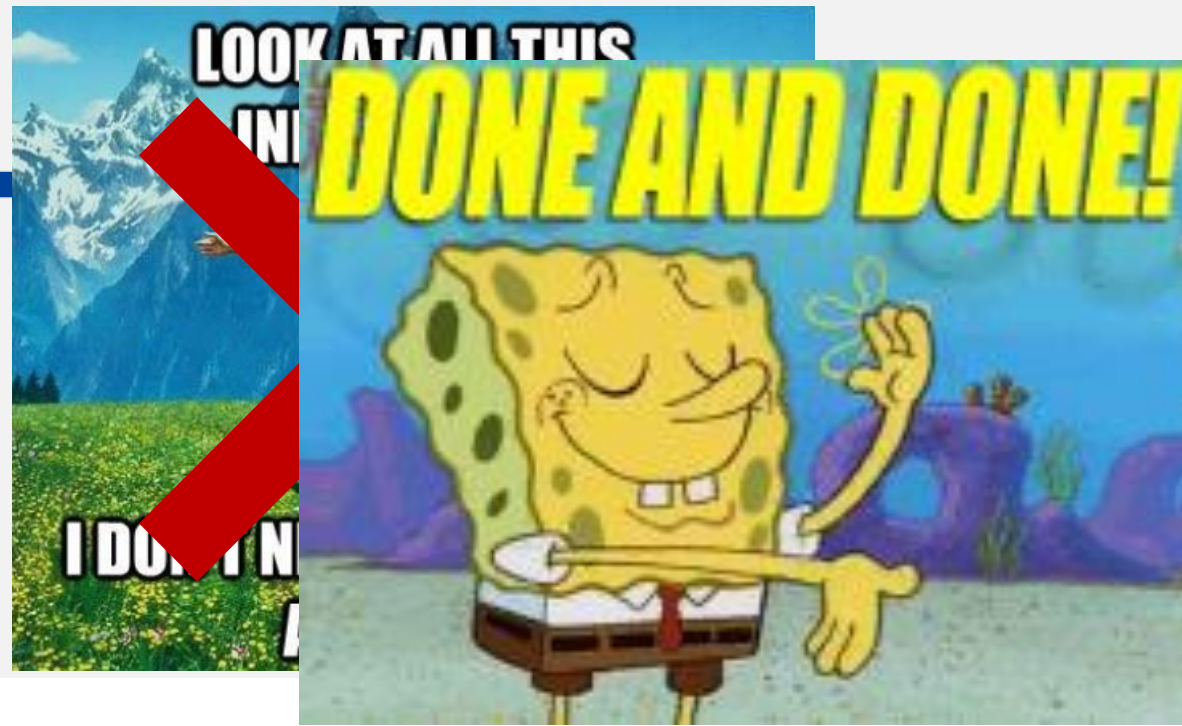
# Review

## Part 1: Hackers

- What is a hacker
- What hackers look like and where they live
  - Russia
  - Ukraine
  - China
  - United States
- How much money hackers make
- Attacks Hackers are using
- What Hackers want from you
- Why they want our personal information

# Review

## Part 2: Cybersecurity Basics – 4 action vectors

1. **Web Applications:**
- Expansion of Cloud Computing
- Developers
  - OWASP Top 10
  - Encrytion
  - Web Application Firewalls
- Everybody
  - Secure Links
  - Mobile Devices
  - Due Diligence
  - Skepticism

2. **Email:**
- Phishing
- Watch for red flags

- Favicons
- Phishing training
- SPF, DKIM, DMARC

3. **Carelessness:**
- Updating software
- Passwords & MFA
- Physical security

4. **Ransomware:**
- Network segmentation
- Backups
- Security fundamentals

# Key Resources

**Web Applications:**
- https://owasp.org/www-project-top-ten/
- https://www.microsoft.com/en-us/security/business/microsoft-intune

**Email:**
- https://www.forbes.com/advisor/business/best-phishing-simulators/
- https://caseworthy.com/articles/a-comprehensive-guide-to-cybersecurity-training-in-human-services
- https://www.mimecast.com/content/dkim-spf-dmarc-explained/
- https://mxtoolbox.com/dmarc/dmarc-email-tools

**Carelessness:**
- https://www.techtarget.com/searchenterprisedesktop/tip/12-best-patch-management-software-and-tools
- https://www.darkreading.com/identity-access-management-security/nist-drops-password-complexity-mandatory-reset-rules
- https://www.alliancetech.com/crack-password/

**Ransomware:**
- https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf
- https://www.cisa.gov/news-events/news/protecting-against-ransomware
- https://www.cisa.gov/resources-tools/resources/cisa-multi-state-information-sharing-and-analysis-center-ms-isac-joint-ransomware-guide
- https://cloud.google.com/beyondcorp

# Books & Blogs

**Books:**

- Krebs, B. (2014). *Spam Nation.*
- Levy, S. (2010). *Hackers: Heroes of the Computer Revolution.*
- Mitnick, K., Simon, W. (2011). *Ghost in the Wires.*
- Zetter, K. (2021). *Countdown to Zero Day.*

**Blogs:**

https://caseworthy.com/resources/

- CSAM Week 1:  https://caseworthy.com/articles/cybersecurity-fundamentals-and-the-users-role/
- CSAM Week 2: https://caseworthy.com/articles/understanding-phishing-a-persistent-cyber-threat/
- CSAM Week 3: https://caseworthy.com/articles/mobile-device-security-and-social-media-how-to-not-get-hacked/
- CSAM Week 4: https://caseworthy.com/articles/how-to-surf-the-internet-safely-without-losing-your-sanity/
- Training: https://caseworthy.com/articles/a-comprehensive-guide-to-cybersecurity-training-in-human-services
- Disabilities: https://caseworthy.com/articles/how-caseworthys-supporting-employees-with-disabilities/

# Links

- https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev
- https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
- https://www.sciencespo.fr/recherche/en/news/where-do-cyber-threats-come-from/
- https://cyberdefensereview.army.mil/Portals/6/Documents/2024_Spring/Jackson_CDRV9N1-Spring-2024.pdf
- https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-is-on-the-front-lines-of-global-cyber-security/
- https://therecord.media/ukraine-cyberattacks-aiding-ground-war-russia
- https://www.brookings.edu/articles/russia-ukraine-and-organized-crime-and-illicit-economies-in-2024/
- https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china
- https://www.sandboxx.us/news/the-man-who-stole-americas-stealth-fighters-for-china/
- https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months
- https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating
- https://cyberscoop.com/potent-youth-cybercrime-ring-made-up-of-1000-people-fbi-official-says
- https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
- https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
- https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/
- https://www.statista.com/statistics/1107206/average-number-of-connected-devices-us-house/
- https://www.verizon.com/business/resources/reports/dbir
- https://techreport.com/statistics/cybersecurity/password-reuse-statistics/
- https://www.sangfor.com/blog/cybersecurity/defining-ai-hacking-rise-ai-cyber-attacks/
- https://ir.zscaler.com/news-releases/news-release-details/zscaler-research-finds-60-increase-ai-driven-phishing-attacks
- https://ipdefenseforum.com/2024/03/u-n-report-north-korea-financing-weapons-program-with-cybercrime/
- https://www.alliancetech.com/crack-password/
- https://www.techtarget.com/searchenterprisedesktop/tip/12-best-patch-management-software-and-tools

# THANK YOU!

We will take a few
minutes for Q&A

CaseWorthy™

**Shayne Champion**

CISO

———————

schampion@caseworthy.com

https://www.linkedin.com/in/shaynechampion

@TNfoSec