



THE CHANGING FACE OF CYBERSECURITY & THE IMPACT ON PROJECT MANAGEMENT

Dave Hatter, CISSP, CCSP, CSSLP, Security +, Network+, PMP, PMI-ACP, ITIL V3

Cyber Security Consultant

Intrust IT

[linkedin.com/in/davehatter](https://www.linkedin.com/in/davehatter)

twitter.com/davehatter

www.youtube.com/user/davidlhatter

A man in a blue suit is standing on a stage to the left of a large projection screen. The screen displays two lines of bold, black, sans-serif text. The stage has a dark floor and is flanked by vertical light bars with glowing orange lights.

**WE ARE NO LONGER
SECURING COMPUTERS**

WE ARE SECURING SOCIETY.

My goals for today

- Educate you
- Motivate you
- Provide actionable advice



PERFECTLY TIMED PHOTOS.COM



INTENT TO KILL | 4:50 PM by VICTOR TANGERMANN

Homeland Security Warns of Cyberattacks Intended to Kill People

"The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us."



Ripped from the headlines...

CPO
MAGAZINE

HOME NEWS INSIGHTS RESOURCES

CYBER SECURITY NEWS 3 MIN READ

Majority of Businesses Unprepared for Reputational Damage and Lawsuits Stemming From Technology Risks

Disconnect Between Legal and Cybersecurity Departments Is Common

SCOTT IKEDA · FEBRUARY 1, 2021

ComputerWeekly.com

IT Management Industry Sectors Technology Topics

Cyber insurance costs up by a third

The frequency and severity of ransomware attacks is a leading factor behind a substantial increase in the cost of obtaining cyber security insurance



By Alex Scroxton, Security Editor

Published: 06 Jul 2021 12:45

Dark Reading Network Computing About Us

DARKReading

SIGN UP FOR OUR NEWSLETTERS

Authors Slideshows Video Tech Library University Security Now Calendar Black Hat Net

THE EDGE ANALYTICS ATTACKS / BREACHES APP SEC CLOUD ENDPOINT IoT OPERATIONS PEI

VULNERABILITIES / THREATS

4/13/2020
10:00 AM

Cybercrime May Be the World's Third-Largest Economy by 2021

techradar pro IT INSIGHTS FOR BUSINESS UK Edition

News Security Web hosting VPN Website builder Features

Cybercrime apparently cost the world over \$1 trillion in 2020

By Barclay Ballard February 15, 2021

That's equivalent to 1% of global GDP

VIDEOS WINDOWS 10 5G IOT CLOUD

zdNet

MUST READ: Big data has a trust issue. This city wants to take a smarter approach

PART OF A ZDNET SPECIAL FEATURE: WORKING FROM HOME: THE FUTURE OF BUSINESS IS REMOTE

Working from home causes surge in security breaches, staff 'oblivious' to best practices

The coronavirus pandemic is thought to be at the heart of a rise in security incidents this year.

CNBC

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV

Cyberattacks now cost small companies \$200,000 on average, putting many out of business

PUBLISHED SUN, OCT 13 2019-10:30 AM EDT

The Register

Here's how crooks will use deepfakes to scam your biz

Need some tools of deception? GitHub's got 'em

Jessica Lyons Hardcastle

Wed 28 Sep 2022 // 07:24 UTC

hashedout by The SSL Store

About Us Resource Library

The FBI reports that direct deposit change requests increased more than 815% in 1.5 years

Ripped from the headlines...

CPO
MAGAZINE

HOME NEWS INSIGHTS RESOURCES

CYBER SECURITY NEWS • 5 MIN READ

New WEF Global Risk Report Names Cybersecurity Challenges as Fourth Greatest Danger to Global Economy

SCOTT IKEDA • JANUARY 29, 2021

TechRepublic SEARCH IT Policy Downloads Coronavirus

Only 31% of Americans concerned with data security, despite 400% rise in cyberattacks

by **Macy Bayern** in **Security**
on June 23, 2020, 9:45 AM PST

Bad actors have flooded the enterprise with coronavirus-related attacks, but professionals working from home have other worries, Unisys Security found.

ZDNet

Nevada school district refuses to submit to ransomware blackmail, hacker publishes student data

ZDNet

First death reported following a ransomware attack on a German hospital



BRIEFING ROOM

FACT SHEET: Act Now to Protect Against Potential Cyberattacks

MARCH 21, 2022 • STATEMENTS AND RELEASES

Fish in a barrel...

"Small and midsized businesses are now the preferred targets for cybercriminals – not because they are lucrative prizes individually but because automation makes it easy to attack them by the thousands, and far too many of them are easy targets."



Most cyberattacks are aimed at small businesses with fewer than 100 employees. Take a moment to learn about best security practices on [#IRS Identity Theft Central: irs.gov/identitytheft #TaxSecurity](#)

Cyberattacks are a serious threat to small businesses. Take action to safeguard your systems and data.



irs.gov/identitytheft

1:02 PM · Jan 18, 2022 · Hootsuite Inc.



Sorry password must contain a special character

System: Enter password:

Me: ScoobyDoo

System: sorry password must contain a special character

Me: ScoobydooFeaturingBatman

Password Change Sign Up sheet

If you'd like to change your password please fill out the form below and we will change your password on the system you indicate.

Full Name	System (Yardi, email, ect.)	Current password	New password
Kyle Smith	Email	Scooter44\$	Sticker442
Dr. Jones	PHONE	89621	4281
Jack H	email	password	password2
Big Ed	facebook	redstep	mimkey
Sam Adams	File Pass		beerlover1791

Come See Me - Shawn

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

Call upper case

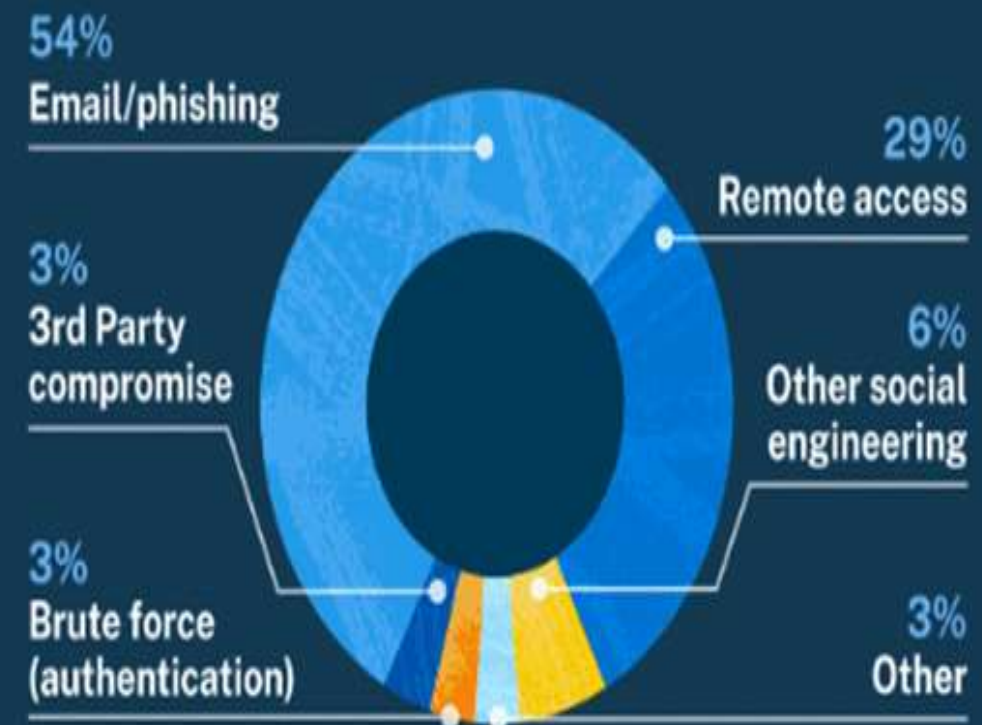
Call upper case

Incidents: By the numbers

Most common cyber incidents (% of reported claims)



Percentage of claims by attack technique



Incidents: By the numbers

The Most Common Types of Cyber Crime

Number of Americans who fell victim to the following types of internet crime in 2021



Source: The FBI's Internet Crime Complaint Center



It's a matter of when, not if...

- "No locale, no industry or organization is bulletproof when it comes to the compromise of data." – Verizon 2016 Data Breach Investigation Report
- "However terrified you are about cybersecurity, you're probably not terrified enough." – LinkedIn Co-founder Reid Hoffman
- Cybercrime is "the greatest threat to every profession, every industry, every company in the world." – Former IBM CEO Ginni Rometty
- "There are two kinds of companies in the United States. There are those who've been hacked ... and those who don't know they've been hacked." – Former FBI Director James Comey

Why is this happening now?

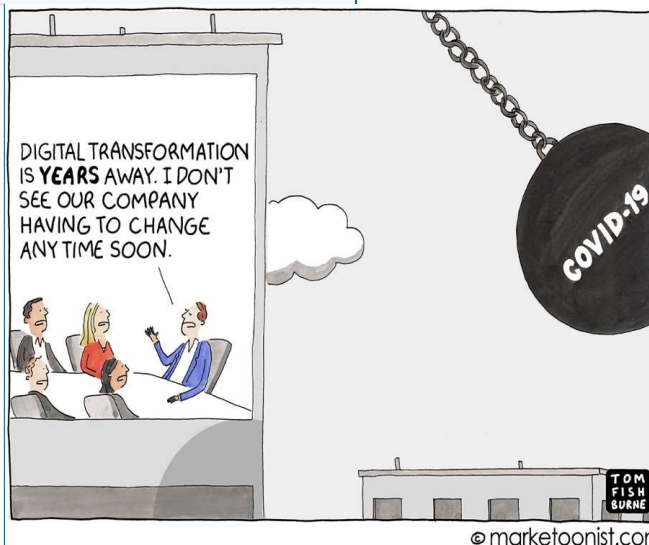


NUMBER OF YEARS IT TOOK FOR EACH PRODUCT TO GAIN 50 MILLION USERS:



Who led the digital transformation of your company?

- A) CEO
- B) CTO
- C) COVID-19



And... The Cloud



KAMATERA
EXPRESS

COMPUTE ▾

[Get Started](#)

[Products & Pricing](#)

[Resources](#)

[Support](#)

Create a Server or two in Hong Kong – for Free

Deploy Your Production, Enterprise-Class Cloud Infrastructure Now

Get Started for Free

30 Day Free Trial



Unlimited
Scale Up and Scale Out

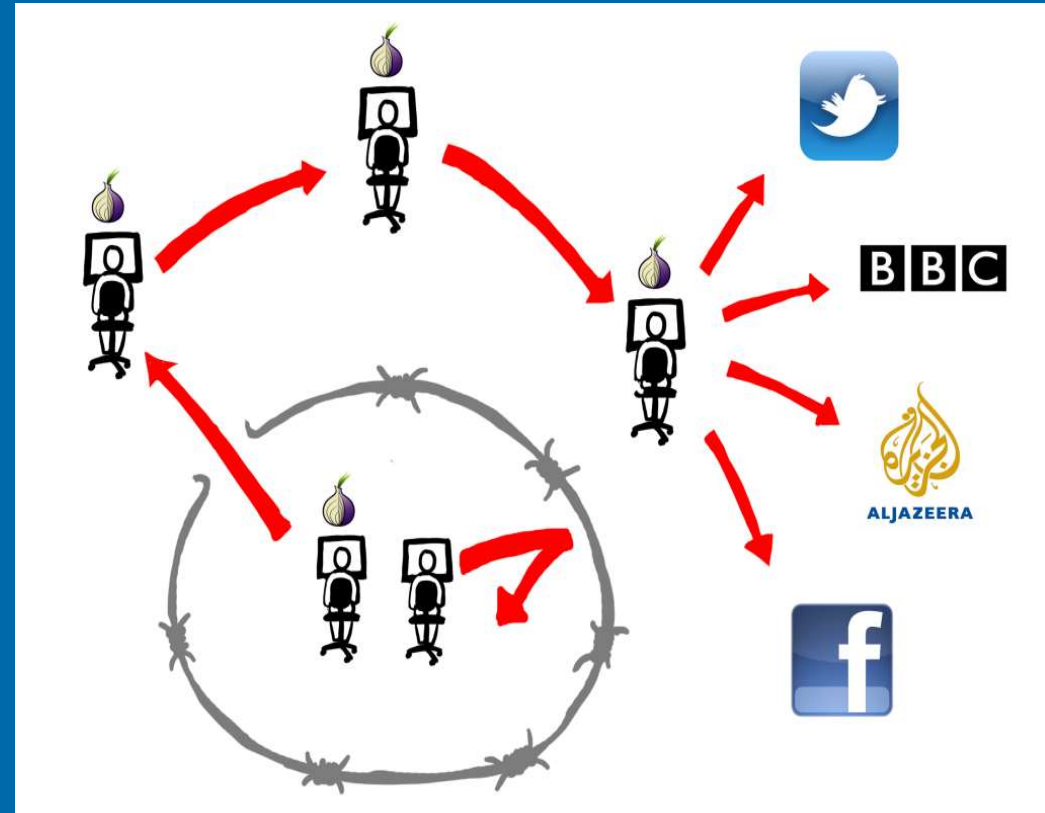
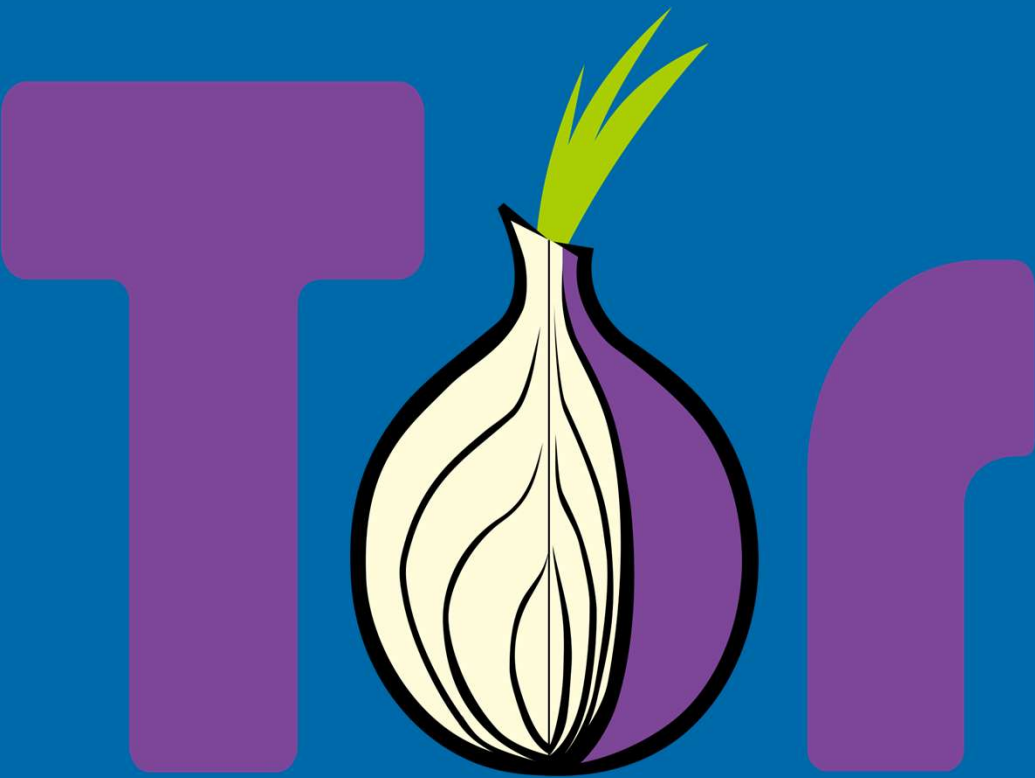


Simple Management
Console and API



Premium
Human Support 24/7

And... Encryption



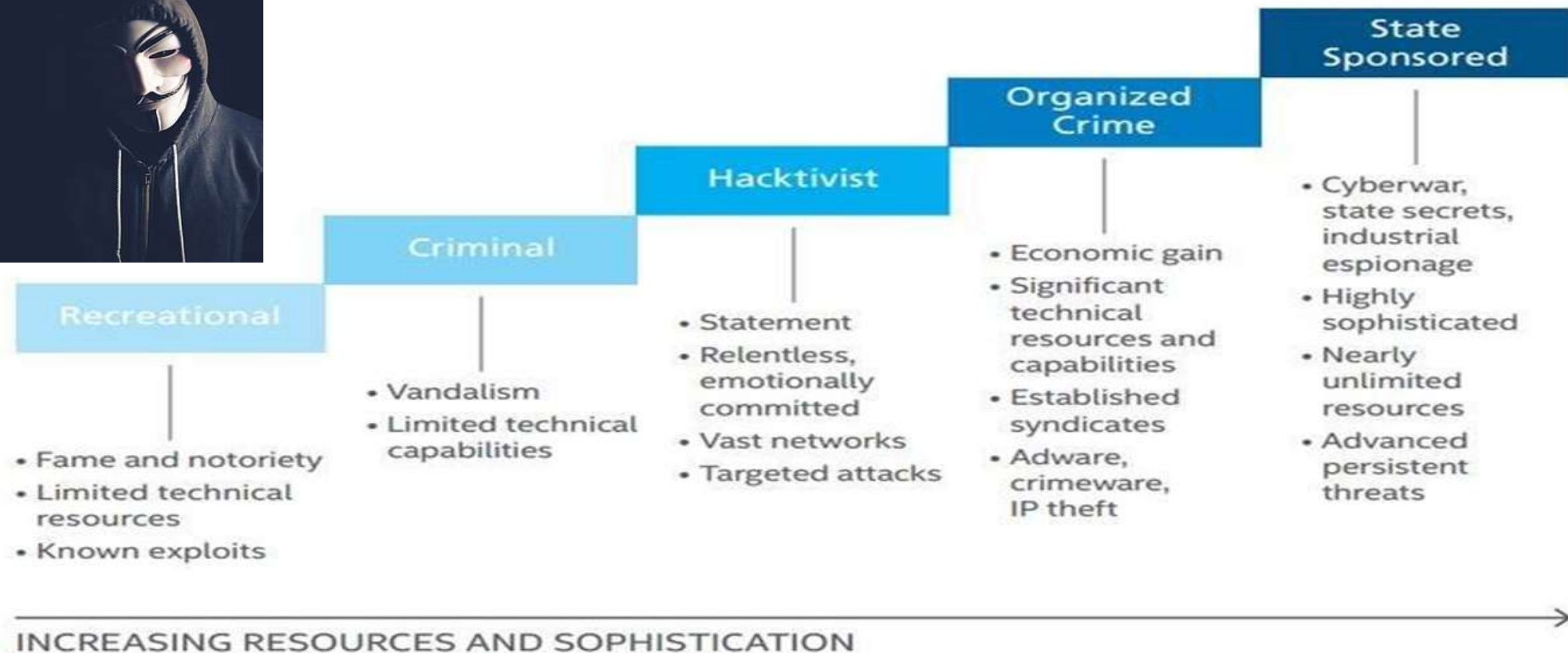
And... Virtual Currency (Crypto)



And... Wide array of threat actors

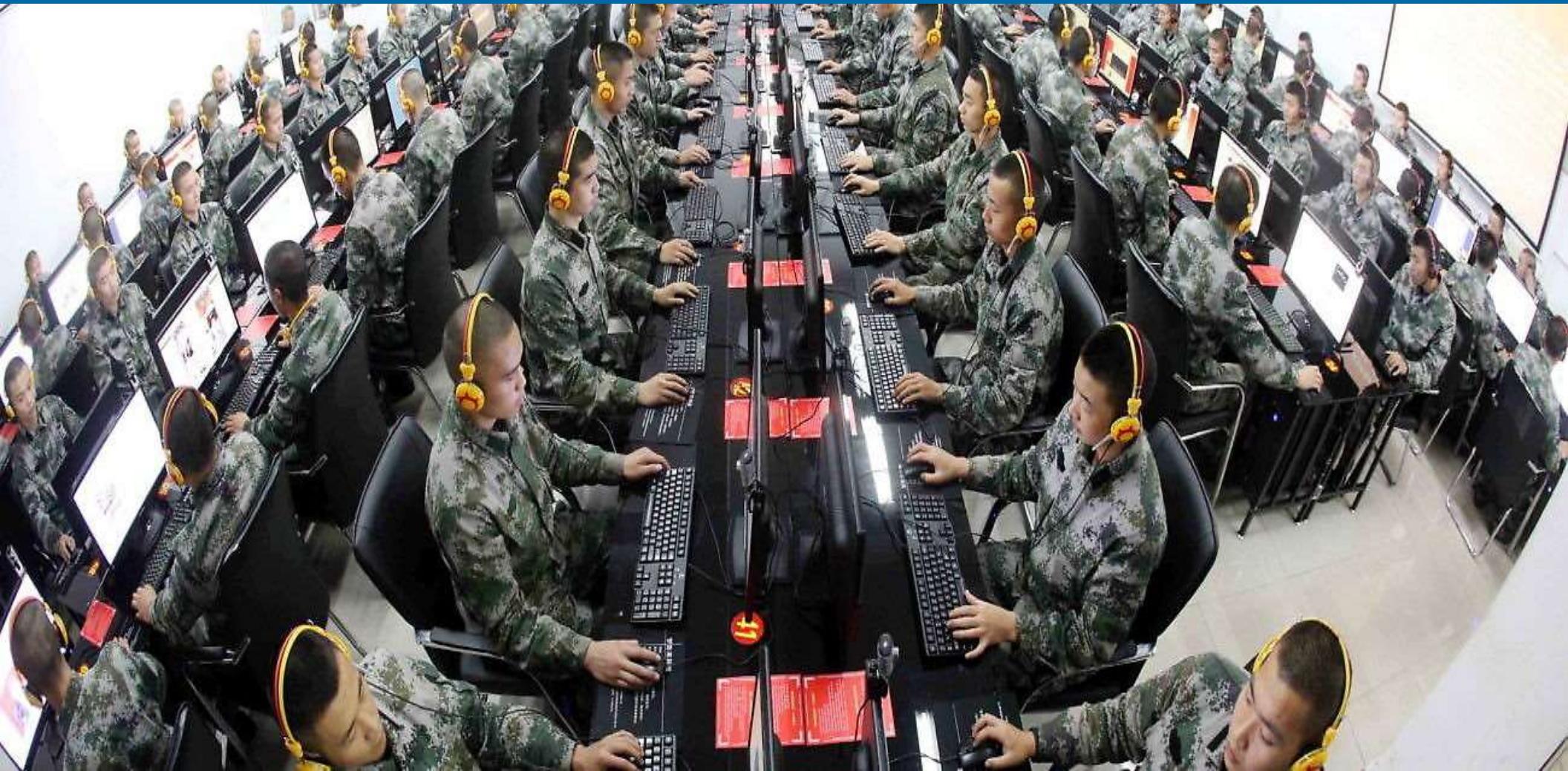


Changing Attacker Profiles



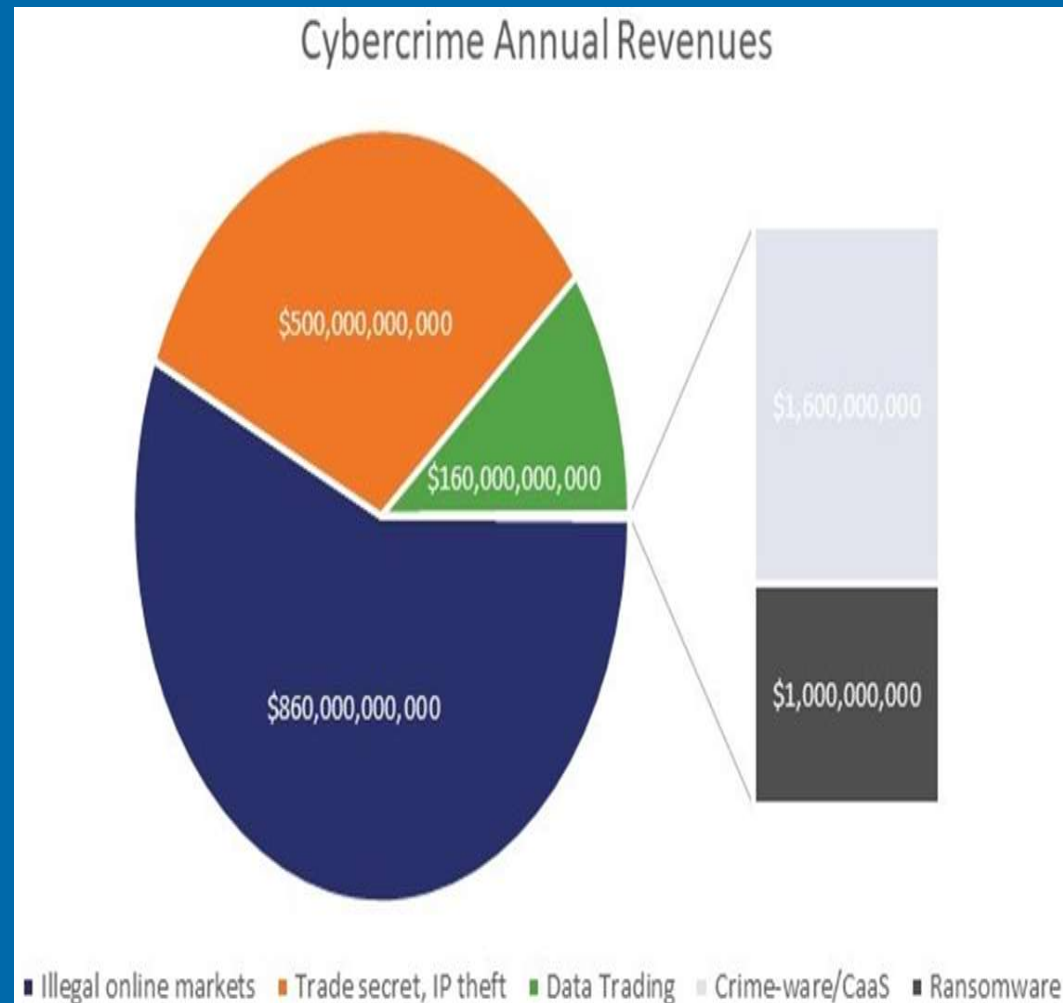
The expansion of attacker types, their resources, and their sophistication.

Nation State Actors (APT's)




And... Crime has gone digital

- Cyberattacks are increasing in frequency, sophistication, impact and cost
- A study by Dr. Michael McGuire puts value of the cybercrime economy at \$1.5 trillion
- Cybercriminals are rarely prosecuted



And... Crime has gone digital



Silk Road
anonymous market


messages 0 orders 0 account \$0.00

Search Go

Shop by Category

- Drugs 6,625
 - Cannabis 1,080
 - Dissociatives 190
 - Ecstasy 829
 - Opioids 382
 - Other 450
 - Precursors 59
 - Prescription 1,429
 - Psychedelics 828
 - Stimulants 1,079
- Apparel 310
- Art 114
- Biotic materials 1
- Books 858
- Collectibles 1
- Computer equipment 43
- Custom Orders 60
- Digital goods 590
- Drug paraphernalia 247

a few words from the Dread Pirate Roberts

Hi,  logout

News

- Closing the Armory
- A brand new look for Silk Road!
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes

Generic XANAX (Alprazolam 1mg): 400 pills Grade A+ \$1.52

Pure Oxycodone HCL Powder (OC, Roxy)- 1/4 \$0.53

TESTOSTERONE CYPIONATE 250mg/ml x 10 \$0.69

25x 130mg MDMA CAPS(FREE SHIPPING) \$1.62

100 GR - MDMA 84%

Pack of Five (5) Suboxone (Buprenorphine) 8mg/2mg

SALE SALE!!!!!! 250 grams METHYLONE!

Bring on the Shadow People! New batch MDPV

CVV.ME

News Billing CVV NO CVV SSN Dumps Cart Orders

GoathFurry71 \$0.00

Search

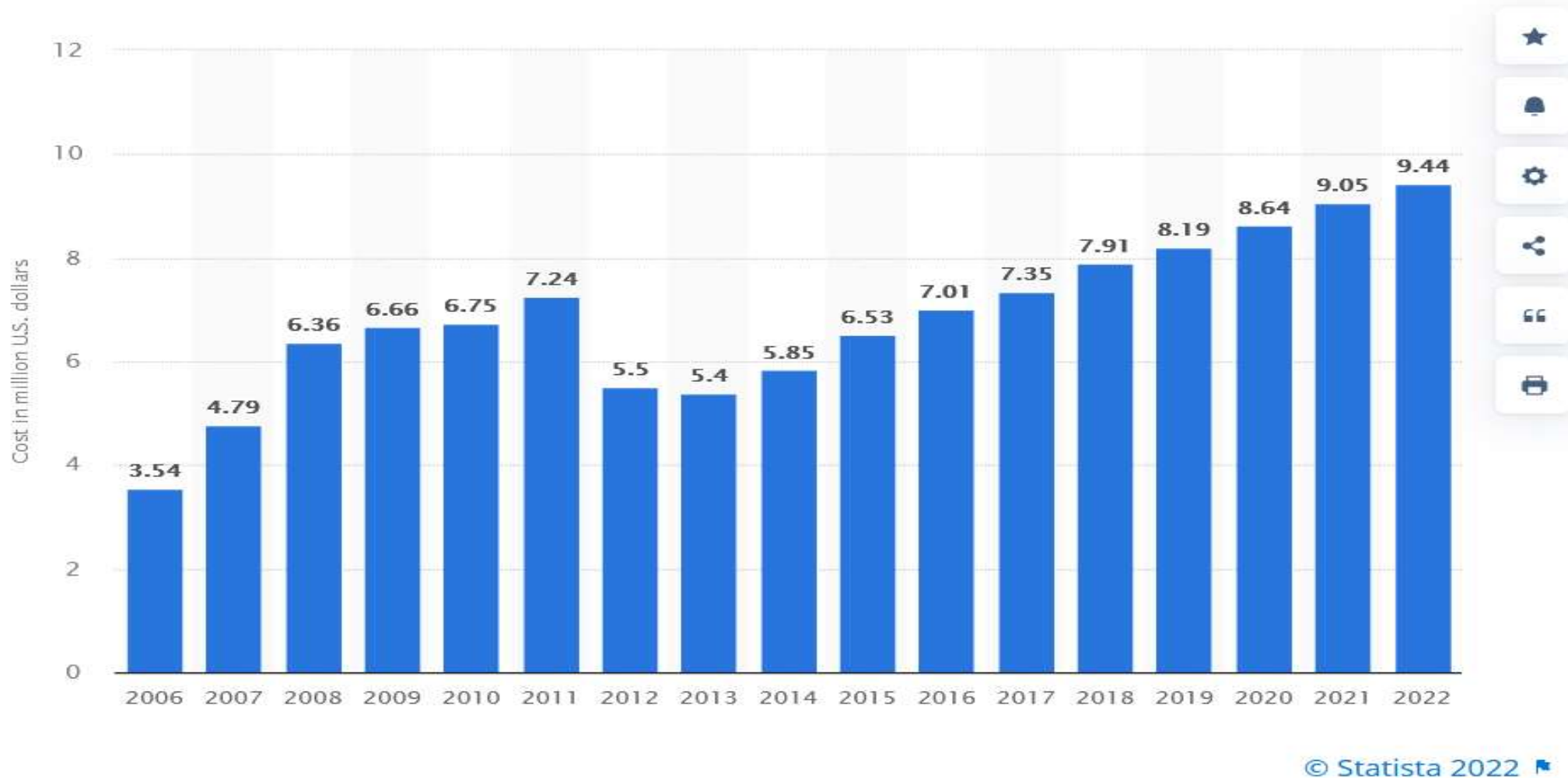
Exp (MM/YY, MMY, MM YY)

SALE DOB SSN FULL Clear

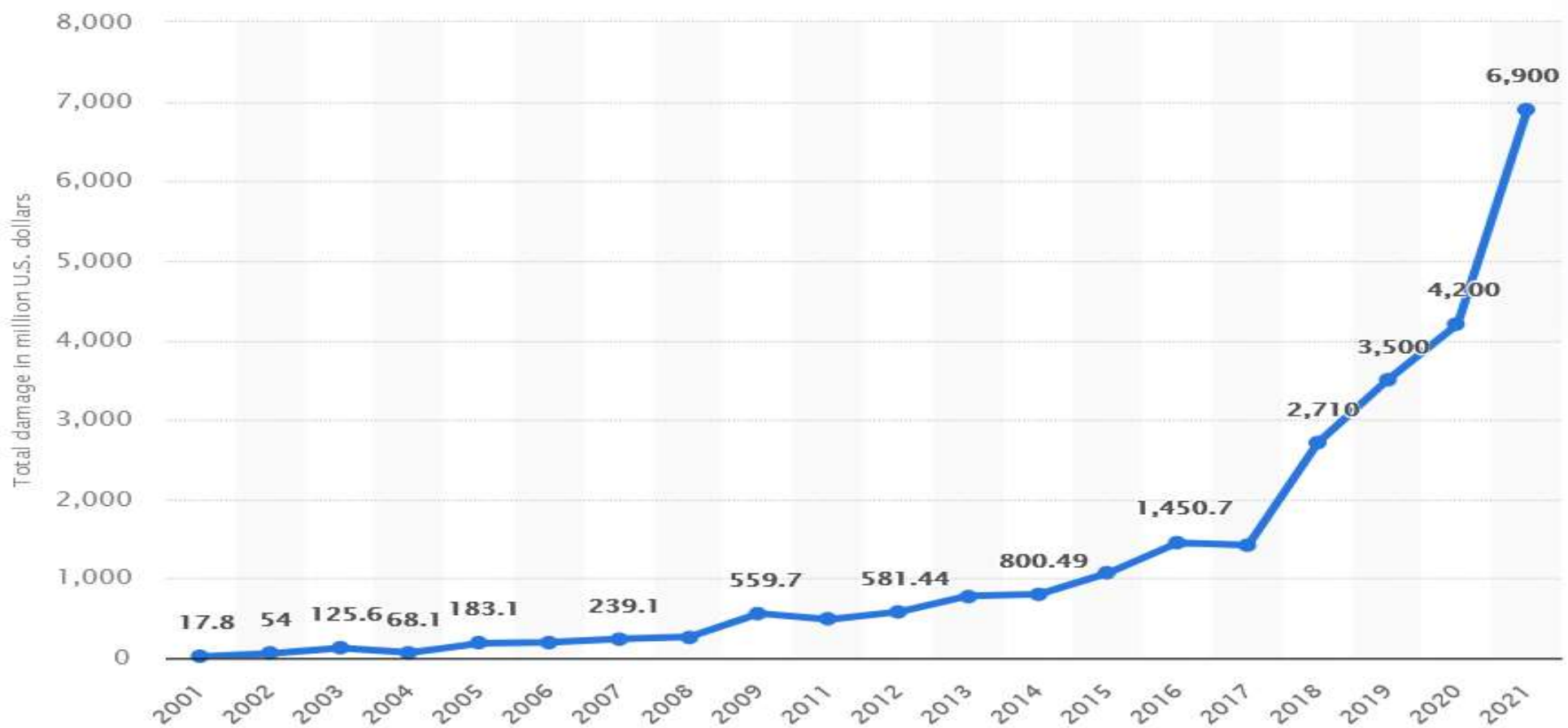
Total 758868 cards found

Bin	Exp	Name	City	State	ZIP	Country	Price	Bank	Base	Valid rate
6011420	12/19	Daniel	Fort wayne	IN	46807	United States	\$9.99	BANK OF AMERICA	SUPER-WORLD-MIX(22/2/2018)	100.00%
3723736	02/22	David	Rochester	NY	14623	United States	\$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
3782968	05/18	Kim	Buford	GA	30518	United States	\$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
3767407	02/20	Christopher	Birmingham	AL	35242	United States	\$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4246315	04/19	Lynn	Bronson	Michigan	49028	United States	\$9.99	CHASE BANK USA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4264520	02/18	Mikael	City of industry	California	91789	United States	\$3.00	BANK OF AMERICA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4246315	08/21	Ben	Huntington beach	California	92647-2	United States	\$9.99	CHASE BANK USA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5567092	04/20	Thomas	Spring arbor	Michigan	49283	United States	\$9.99	CITIBANK, N.A.	SUPER-WORLD-MIX(22/2/2018)	100.00%
4006138	11/18	Michael	Lake zurich	IL	60047	United States	\$9.99	U.S. BANK NATIO...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5594940	09/20	Daicel	Beaver dam	KY	42320	United States	\$9.99	N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
4715291	11/20	Steve	West chicago	IL	60185	United States	\$9.99	BANK OF AMERICA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
6011398	03/19	Trudy	Binghamton	NY	13901	United States	\$9.99	BANK OF AMERICA	SUPER-WORLD-MIX(22/2/2018)	100.00%
5569206	04/20	Eric	North royalton	OH	44133	United States	\$9.99	COMERICA BANK	SUPER-WORLD-MIX(22/2/2018)	100.00%
4147202	11/22	Aaron	Hamilton	OR	97405	United States	\$9.99	CHASE BANK USA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4100400	01/21	John	Commerce twp.	MI	48390	United States	\$9.99	N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
4427420	06/20	Kyle	Norman	OK	73072	United States	\$7.99	JPMORGAN CHASE ...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5597080	02/21	Tooling	Eaton	Ohio	45320	United States	\$9.99	N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
5475030	08/19	Fa	Bleiswijk	chanks	2665	Netherlands	\$17.99	COOPERATIEVE CE	SUPER-WORLD-MIX(22/2/2018)	100.00%

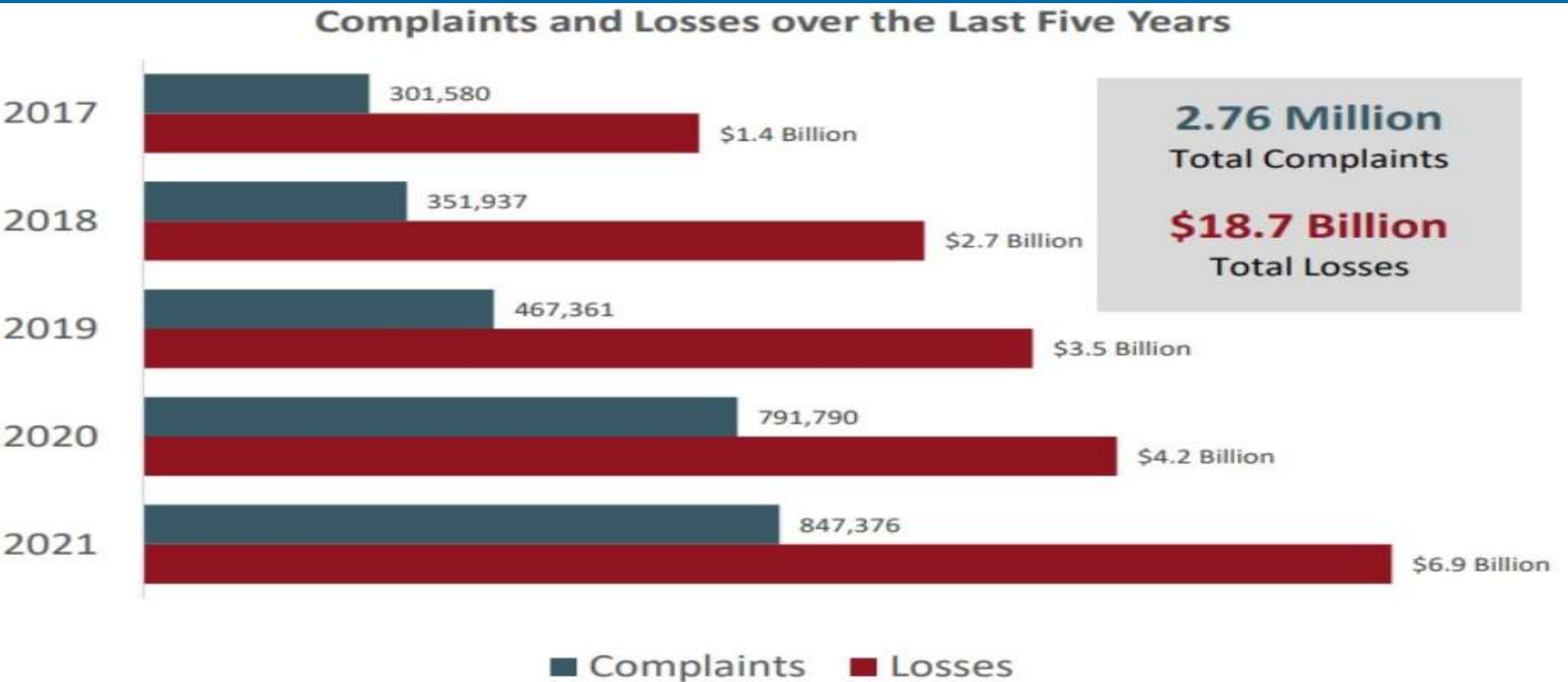
Cybercrime costs incurred per IC3



Cybercrime damage in \$ per IC3



Cybercrime damage in \$ per IC3



Cybercriminal Complaints and Losses Between 2017-2021 | Source: [FBI IC3](#)

Cybercrime costs

Figure 6. Costs of a data breach

Above the surface: Well-known cyber incident costs

1. Customer breach notifications
2. Post-breach customer protection
3. Regulatory compliance (fines)
4. Public relations/crisis communications
5. Attorney fees and litigation
6. Cybersecurity improvements
7. Technical investigations

Below the surface: Hidden or less visible costs

1. Insurance premium increases
2. Increased cost to raise debt
3. Operational disruption or destruction
4. Lost value of customer relationships
5. Value of lost contract revenue
6. Devaluation of trade name
7. Loss of intellectual property

Source: "Beneath the surface of a cyber attack: A deeper look at business impacts," Deloitte Cyber Risk Services.

Cybercrime costs are rising

- Average incident response cost hovers around \$420,000, with cyber forensics accounting for about 40% - Chubb
- Data breach costs are expected to reach \$5 trillion by 2024
- 60-70% of claims involve breaches of less than 100 data records
- Even a small breach can cost substantial amounts of money

PERSONALLY IDENTIFIABLE INFORMATION (PII)
BREACH

*** RECEIPT ***
250 RECORDS EXPOSED

INCIDENT INVESTIGATION

BREACH COACH	\$25,000.00
FORENSICS	\$60,000.00

NOTIFICATION & CRISIS MANAGEMENT

CRISIS MANAGEMENT	\$30,000.00
NOTIFICATION	\$2,800.00
CALL CENTER	\$1,300.00
CREDIT MONITORING	\$225.00

INCIDENT INVESTIGATION SUBTOTAL \$85,000.00
NOTIFICATION & CRISIS MANAGEMENT SUBTOTAL \$34,325.00

TOTAL AMOUNT \$119,325.00



And... Data is increasingly valuable

Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for:



Social security number



\$1

Online payment services login info
(e.g. Paypal)



\$20-\$200

Credit or debit card
(credit cards are more popular)



\$5-\$110

With CVV number
\$5

With bank info
\$15

Fullz info*
\$30

Drivers license



\$20

Loyalty accounts



\$20

General non-financial institution logins



\$1

Diplomas



\$100-\$400

Passports (US)



\$1000-\$2000

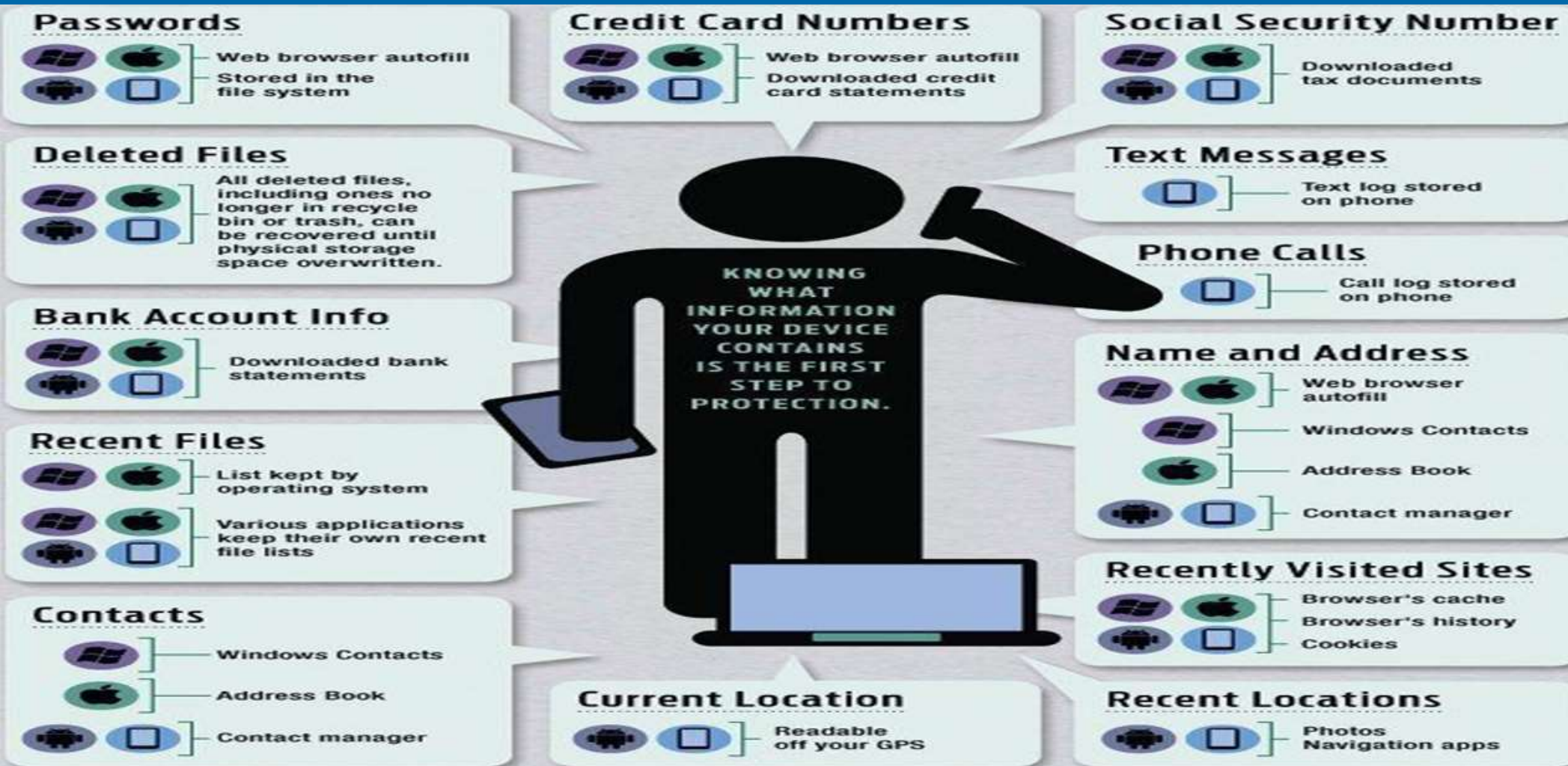
Subscription services

\$1-\$10

Medical records

\$1-\$1000**

And... Surveillance capitalism



And... The attack surface grows daily



THE EXPLOSION OF IOT DEVICES

**30.73
BILLION**





IoT devices expected by 2020*

**75.44
BILLION**

IoT devices expected by 2025

AN EASY TARGET

IoT devices are inherently vulnerable and relatively easy to hijack. Why?

-  They're leaving security up to the owner
-  They're not regularly patched
-  They're not running security software
-  They're not designed with security in mind



EVERYTHING IS CONNECTED!

IoT devices are in our homes and offices, and on our bodies



22 Million

Amazon Echos sold in 2017*



1 Per Second

how often Google says it has sold a Google Home device since October 2017*



\$310.4 Million

wearable devices sales in 2017*

And... People remain the weakest link

Login: admin
Password: admin



- 
- A knight in full plate armor, including a helmet with a visor, stands in a forest. He holds a sword with both hands, the blade pointing upwards. The armor is highly detailed with rivets and a chainmail collar. The background is a blurred forest scene.
- Defense in Depth
 - Patched systems
 - 24/7 monitoring/alerting
 - Annual compliance auditing
 - Experienced IT/Security team



A knight in full plate armor, including a helmet with a visor, stands in a forest. He holds a sword with both hands, the blade pointing upwards. The armor is highly detailed with rivets and a chainmail collar. The background is a blurred forest scene.

*User clicks on
an email*

Cybersecurity myths

- My organization is too small or insignificant to be a target
- My data (or the data I have access to) isn't valuable
- Attacks are always sophisticated or technically complex
- New software and devices are secure out-of-the-box
- Security is an IT issue

Threats

1



Malware

2



Web-based attacks

3



Phishing

4



Web application attacks

5



Spam

TOP 15 CYBER THREATS



6



DDoS

7



Identity theft

8



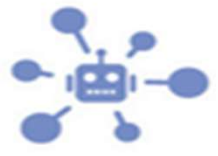
Data breach

9



Insider threat

10



Botnets

11



Physical manipulation, damage, theft and loss

12



Information leakage

13



Ransomware

14



Cyberespionage

15

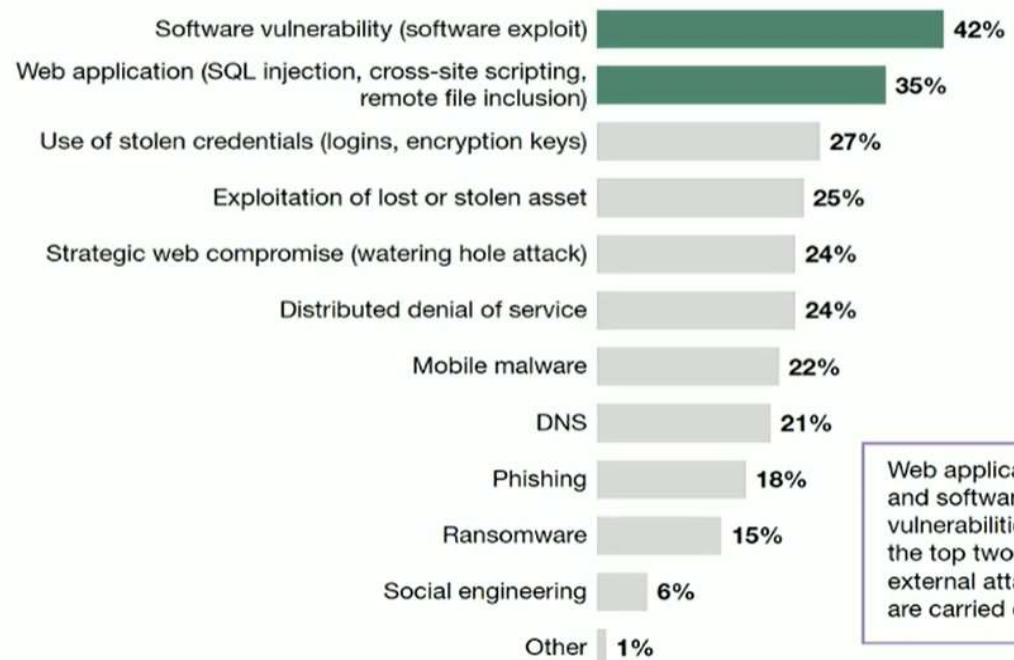


Cryptojacking

Threats

The Prevalence of Breaches and Their Methodology

“How was the external attack carried out?”



Web applications and software vulnerabilities are the top two ways external attacks are carried out.

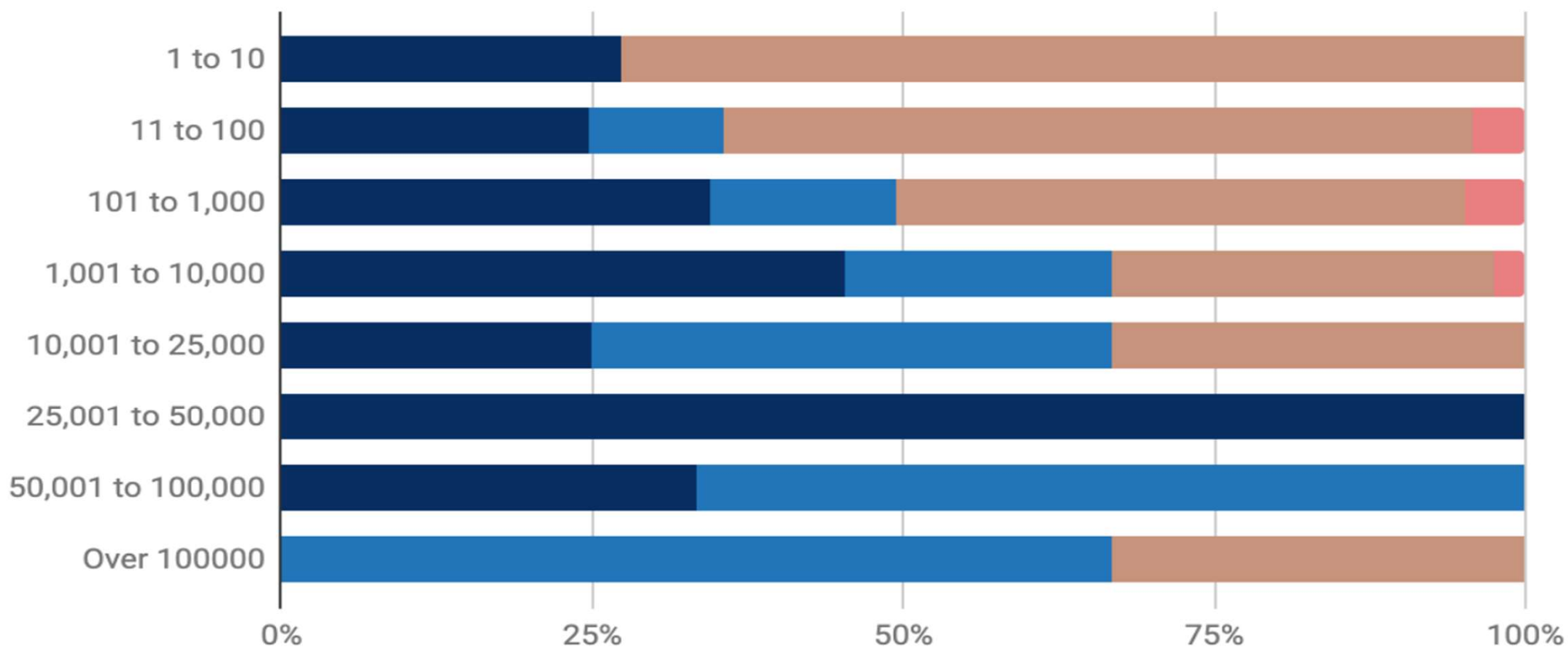
Base: 465 security decision makers with network, data center, app security, or security ops responsibilities who experienced an external attack when their company was breached

Sources: Forrester Analytics Global Business Technographics® Security Survey, 2019

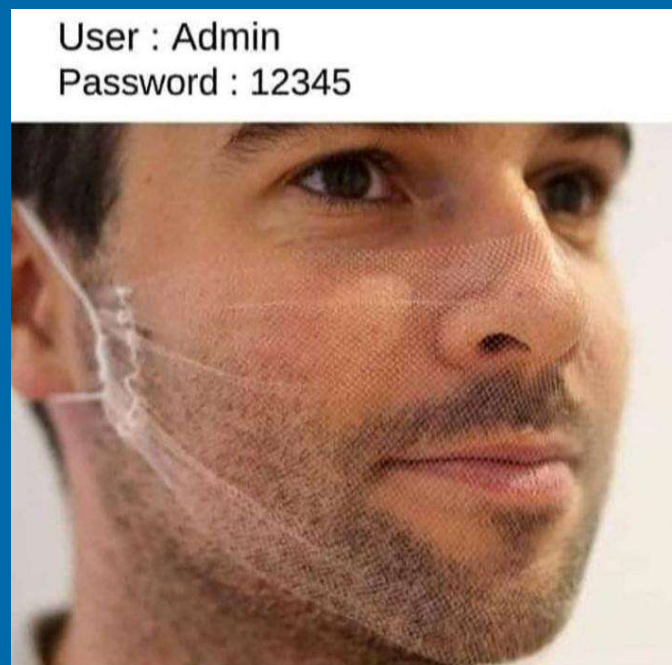
Threats

Attack Vector by Company Size

■ Email Phishing ■ RDP Compromise ■ Software Vulnerability ■ Other



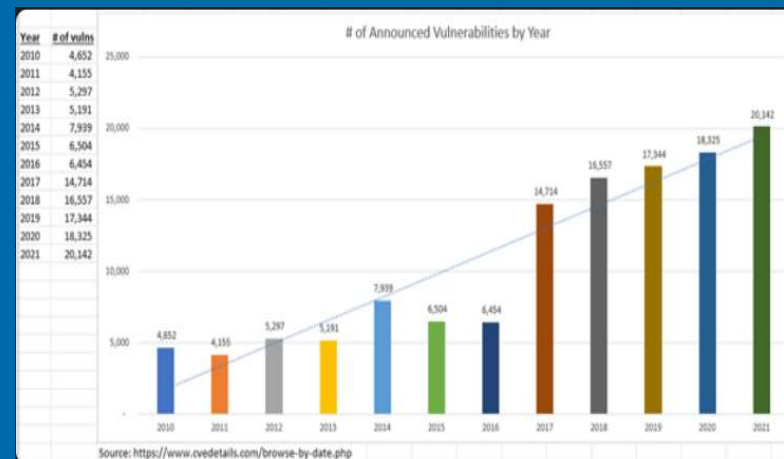
Threats: Poor credential management



A recent Verizon Data Breach Investigations Report says compromised passwords are responsible for 81% of hacking-related breaches

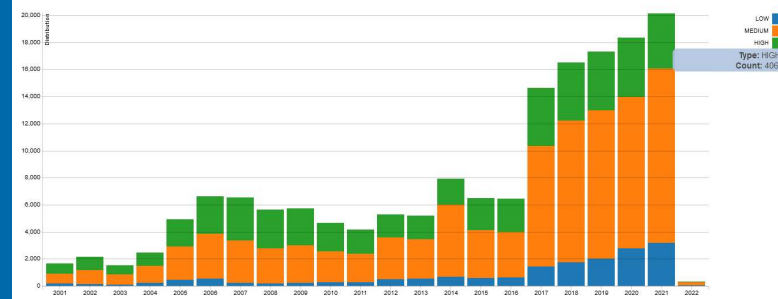
Threats: Unpatched Software

- A Ponemon Institute found 57% of breaches due to unpatched software
- 34% of victims were aware of holes but didn't patch them in time.
- 37% of victims don't perform regular scans to find vulnerabilities
 - Patching gaps are an issue:
 - Some unaware of available updates
 - Some are aware but don't have the resources or strategies to implement patches



CVSS Severity Distribution Over Time

This visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score. For more information on how this data was constructed please see the NVD CVSS page .

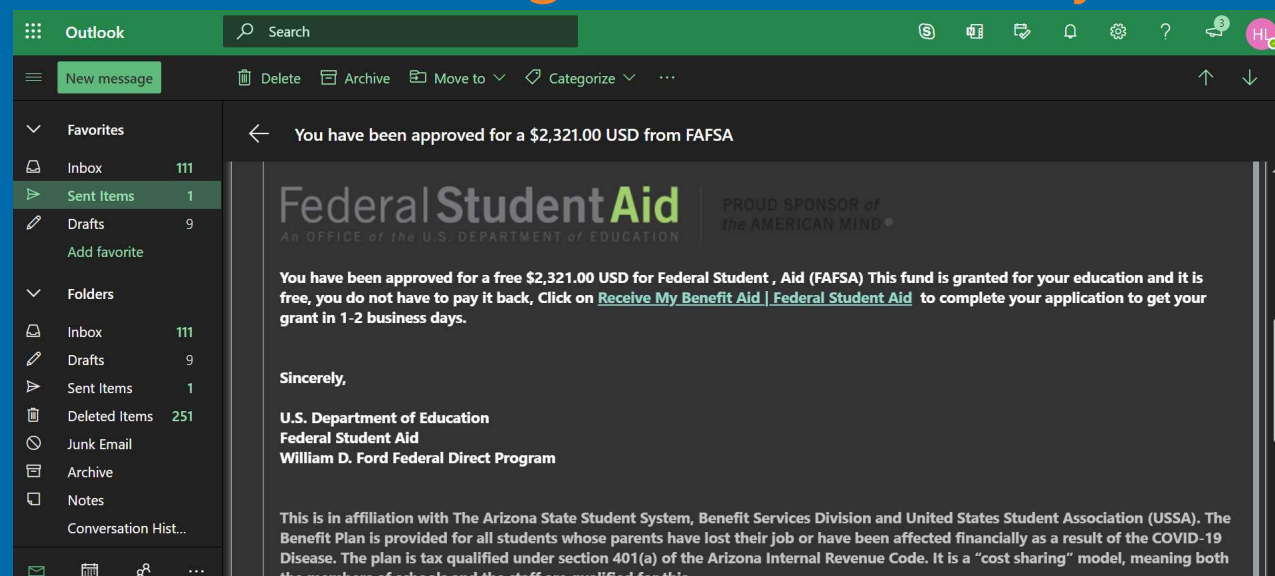


Threats: Spoofing

- "Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security." —

Techopedia

- Spoofing leads to:
 - Phishing
 - Vishing (Voice based)
 - Smishing (Text based)
 - Doppleganger or Lookalike websites



Threats: Deepfakes

This person does not exist ->

Forbes

CYBERSECURITY • EDITORS' PICK

Fraudsters Cloned Company Director's Voice In \$35 Million Bank Heist, Police Find



QS Study

HOME

SUBJECT

TOPIC

Home > Technology > Thieves pulled \$243,000 robbery using an audio Deepfake

— TECHNOLOGY

Thieves pulled \$243,000 robbery using an audio Deepfake

Threats: Phishing

- “Cybercrime in which a target or targets are contacted by **email, telephone or text message** by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.” – Phishing.org
- Types of Phishing include:
 - Spear phishing
 - Whaling
 - Vishing
 - Smishing



Threats: Phishing

From: Dave Hatter <pm772858@gmail.com>

Sent: Wednesday, October 30, 2019 1:23 PM

To: Jeff Bethell <jbethell@fortwright.com>

Subject: Hey Jeff

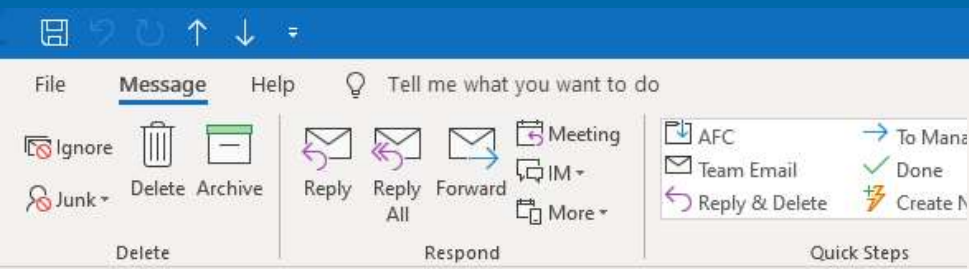
Hey Jeff , i need you to help me get some gift cards at the store right now for some council members / staff appreciation gifts , let me know if you can do that right away because there is a sharp deadline for this request .

Dave Hatter

Mayor

Sent from my mobile device

Threats: Phishing



RE: Divorce papers



Brown & Booth LLP <Booth@brown-booth-law.com>
To: Dave Hatter

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

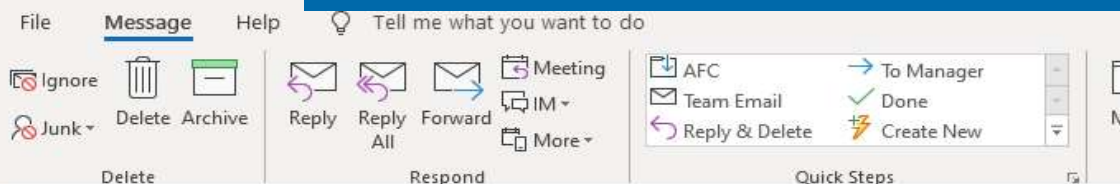
WARNING: This e-mail is from an external sender. Be suspicious of any links or attachments. If you are not expecting this e-mail, or about any type of financial transaction like a wire, call the sender via phone to validate all the information.

Dave

My name is Keith Booth and I am a senior partner at BROWN & BOOTH LLP.
Your spouse has contracted me to prepare the divorce papers.
Here is the first draft, please contact me as soon as possible:

http://www.brown-and-booth-law.com/papers/divorce_Hatter.doc

Thank you
Keith L. Booth



RE: Divorce papers



Brown & Booth LLP <Booth@brown-booth-law.com>
To: Dave Hatter

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

WARNING: This e-mail is from an external sender. Be suspicious of any links or attachments. If you are not expecting this e-mail, or about any type of financial transaction like a wire, call the sender via phone to validate all the information.

Dave

My name is Keith Booth and I am a senior partner at BROWN & BOOTH LLP.
Your spouse has contracted me to prepare the divorce papers.
Here is the first draft, please contact me as soon as possible:

http://www.brown-and-booth-law.com/papers/divorce_Hatter.doc

Thank you
Keith L. Booth



Original URL:
<http://addto.password.land/xywms0aw9upwqnsawnrjnvvybd1orgdhrwnczovl3nlby3cvyzwqtb9naw4ubmv0rl3bhz2vzl2findfly2jknghjnjly2lwawvudf9pzd01ntgxmmdaxmjemy2ftcgfpz25fcnvux2lkpti3mjyyndu=>
Click or tap to follow link.


Threats: Phishing

Re: My photos



Jessica Swanson <jessicas17@yahooo-mail.com>

To  Dave Hatter

 Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Hi Dave,

I think you may have sent this link to me in error...Are you really sure you want to be sharing these kinds of personal photos with everyone?

--

On Tuesday at 9:50 AM, Dave Hatter <Dave.Hatter@intrust-it.com> wrote:

Here are the pics I told you about!

<https://www.flickr.com/users/2jd94l2j38/gallery/>

Talk to you soon.

Dave

<https://cardpayments.microransom.us/xvgpsmfpubfbwwfjxvdjswfdgunvrmuvywjnos01xrm9aemsyzed0dwqytxpumhhlv0uwemnuyzjwm0z6wmpsslrvmxboa1ppu1hsv1duwkppv2rvvfhwalkxwmhkbfxvtbwt2nhmunaekv2uja5bvqzze1xbul4wwtgalf6vjipsei1wlrod1jirmluvghzvdkumvhvmpta1pfukhsvwrysm9lmeuxvvdkvlixce5vmvj1zeu0m2nvdgftvzf2vmpnewvndbtbmrmym1rsm1uzwk5tmvpwwkhwv1zeaelrmljyufmwdgruzdnam1jozfhsa2fuvlrwvgxkvlrkb1neqmxkeja5ls1hmzy1zjjhotbly2njownimguxyzbjyzzlzcynzkyzje4yzfmmmfk?cid=1002096742>

Click or tap to follow link.



Threats: Phishing

JW

Joyce Woods

To: David Hatter; y

Inbox

You replied on 3/3/2016 2:02 PM.

-----Original Message-----

From: Dave Hatter [mailto:dhatter@fortwright.com]

Sent: Wednesday, March 02, 2016 4:09 PM

To: Joyce Woods <jwoods@fortwright.com>

Subject: RE: Question

Thanks for the information. I need you to initiate 2 wire transfers today for an international payment and a local payment also. Let me know what information is required.

Sent from my iPhone

Sorry Dave,

I just got your message. I have been working on other things. If you mean the General Fund Checking Acct. the balance today is \$4,265,408.72.

Joyce

From: Dave Hatter [mailto:dhatter@fortwright.com]

Sent: Wednesday, March 02, 2016 12:35 PM

To: Joyce Woods <jwoods@fortwright.com> <mailto:jwoods@fortwright.com>

Subject: Question

Are you available? I need to ask you a quick question What is the present balance in the operating checking account? Reply as soon as possible.

Sent from my iPhone

JW

Joyce Woods

To: David Hatter; y

From: Dave Hatter [mailto:dhatter@fortwright.com]

Sent: Wednesday, March 02, 2016 12:35 PM

To: Joyce Woods <jwoods@fortwright.com>

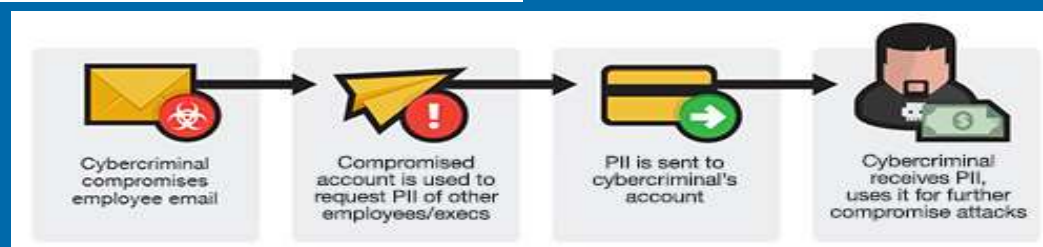
Subject: Question

Are you available? I need to ask you a quick question What is the present balance in the operating checking account? Reply as soon as possible.

Sent from my iPhone

Threats: Business Email Compromise

- BEC is an email-based scam where an attacker gains access to one or more email accounts attempting to fool employees into transferring money or sensitive data.

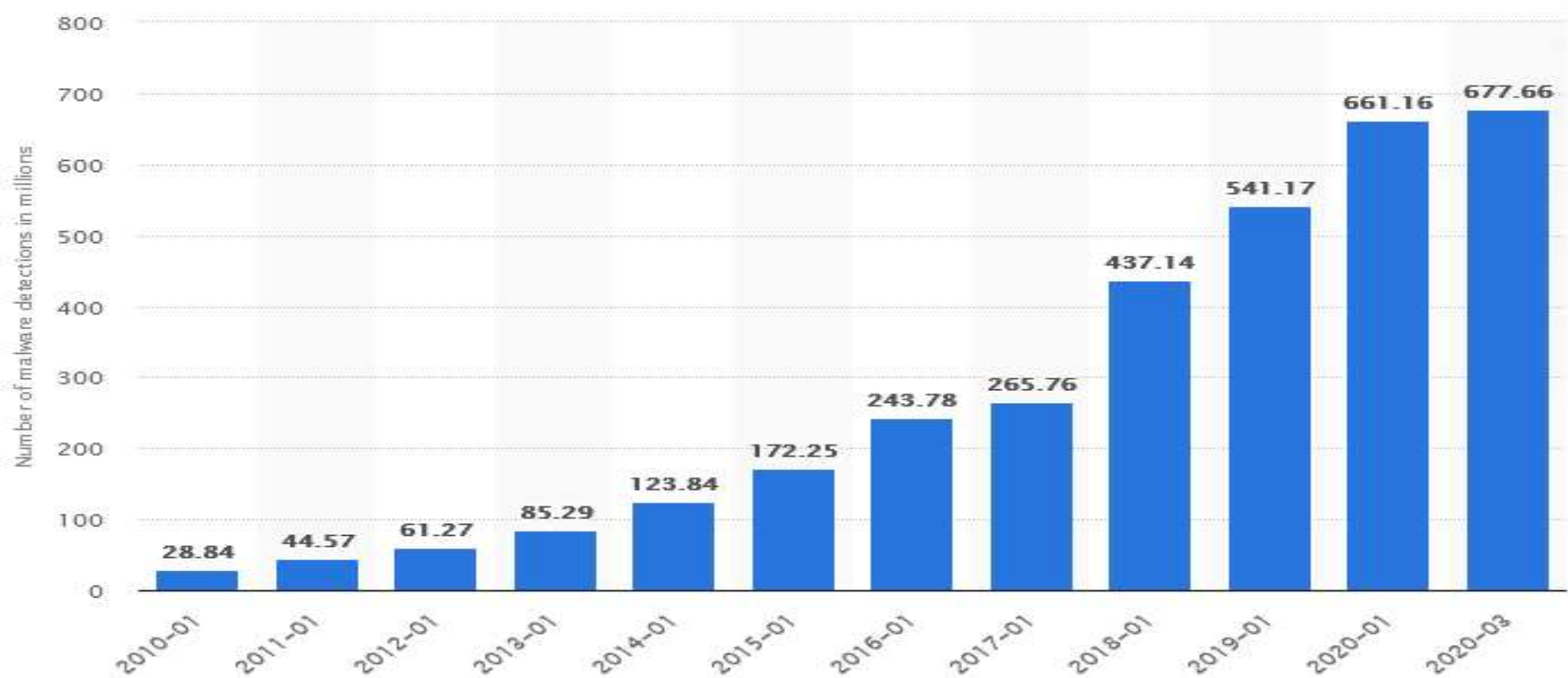


Threats: Malware

- Viruses
- Worms
- Rootkits
- Keystroke Loggers
- Adware
- Bots
- Zombies
- Crypto miners



Malware growth



[Additional Information](#)

© Statista 2021

[Show source](#)

Threats: Ransomware

- Malware that encrypts data and demands a ransom
 - The losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information
 - Ransom demands increased more than 10 times in one year
 - Exfiltration/Doxxing Threat
- Delivered many ways:
 - Phishing
 - Infected web sites
 - Compromised devices
 - Open ports



Threats: Ransomware

Ransomware hit manufacturing, construction the hardest

Number of ransomware cases by sector, Jan. 2020 - July 2022

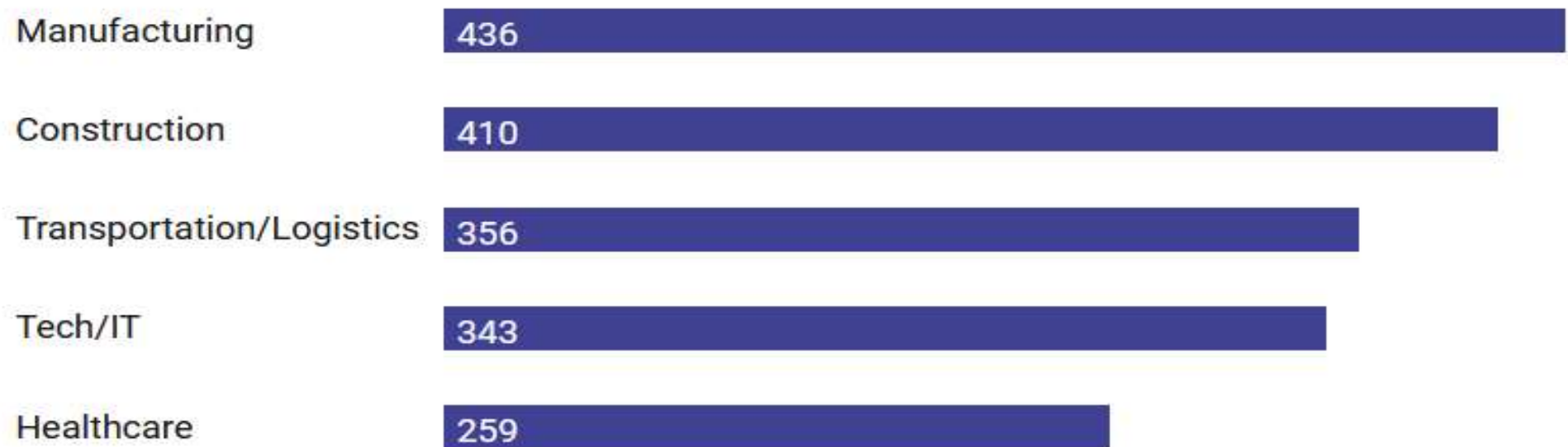


Chart: Naomi Eide • Source: [NordLocker](#) • [Get the data](#) • Created with [Datawrapper](#)

Threats: Public Wi-Fi

- Information can be stolen
- Malware can be planted

Using Public Wi-Fi in a cyber security conference



MIDDLE IN THE MIDDLE ATTACK EXAMPLE

NORMAL CONNECTION



SERVER



CLIENT



MAN IN MIDDLE CONNECTION



SERVER



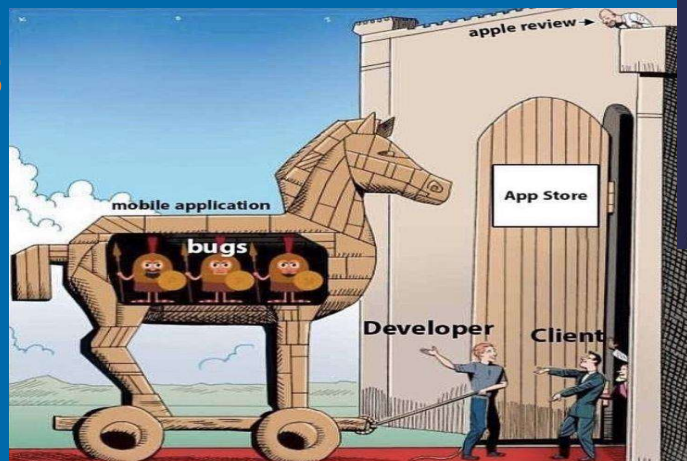
MAN IN THE MIDDLE



CLIENT

Threats: "Free" software

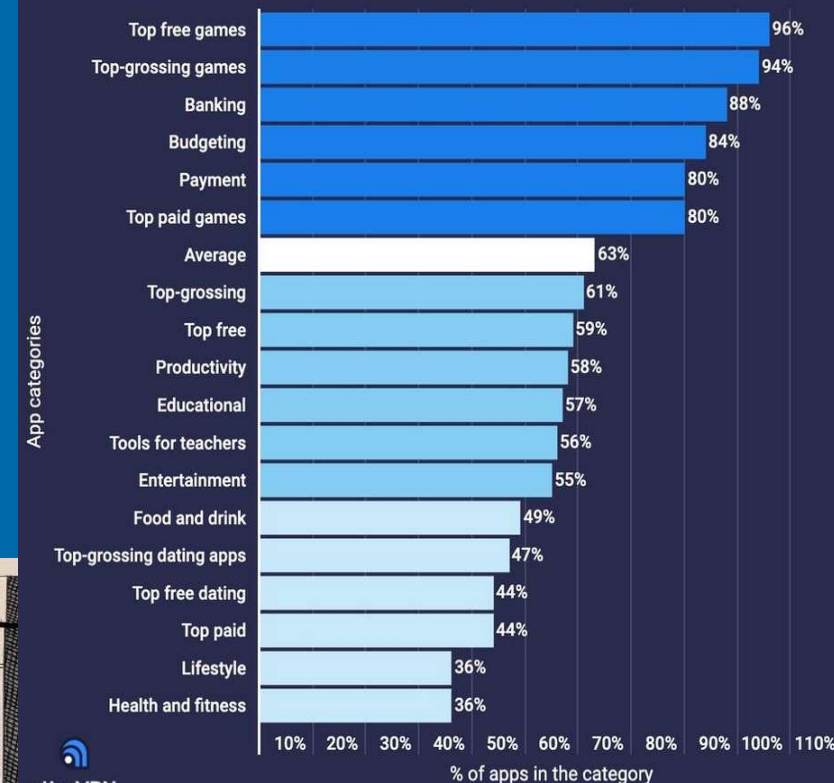
- Many free apps are thinly veiled malware
- 172 malicious apps hosted on Google Play were installed more than 335 million times in September of 2019 and have been found in the Apple store too
- Subscription scams
- Data leakage



Share of Android applications with at least one known vulnerability, by app category (Q1 2021)

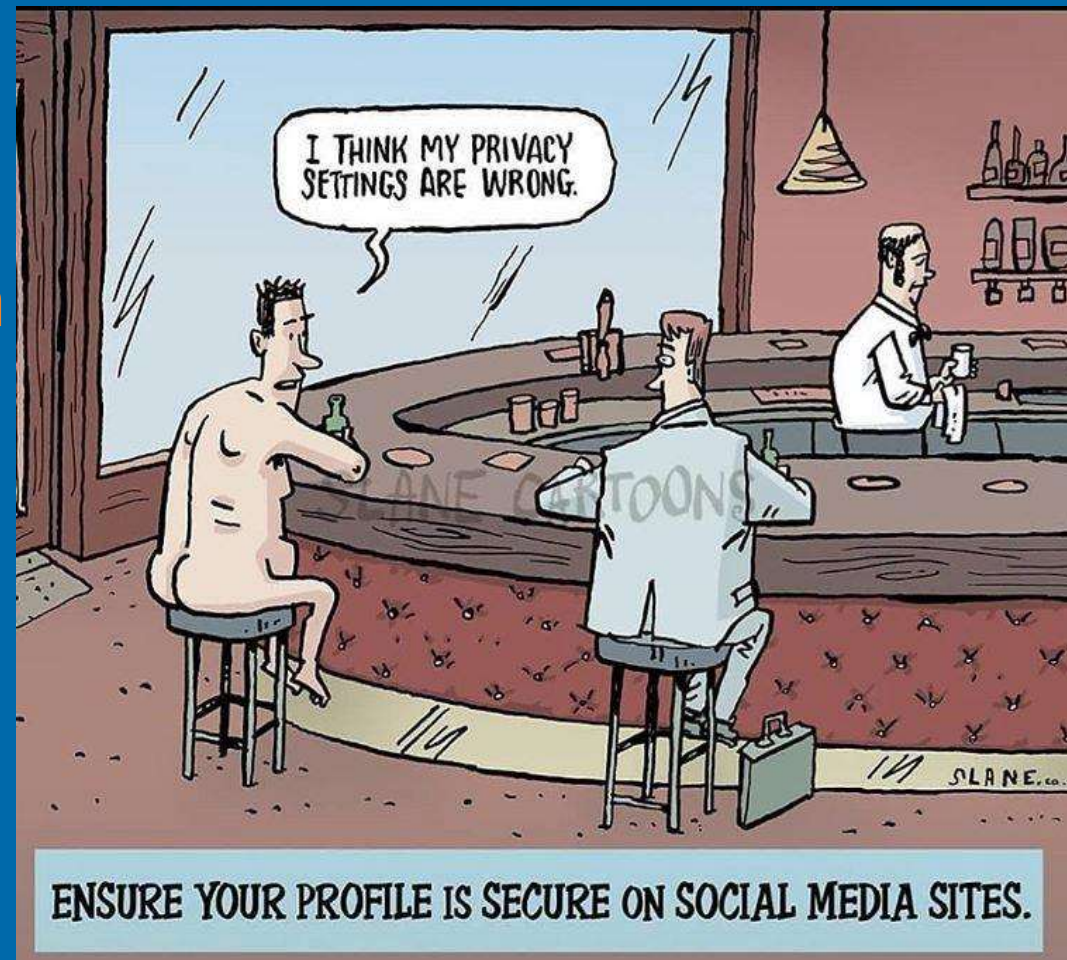


FACT: 63% of Android applications contained security vulnerabilities in Q1 2021, with an average of 39 vulnerabilities per app.



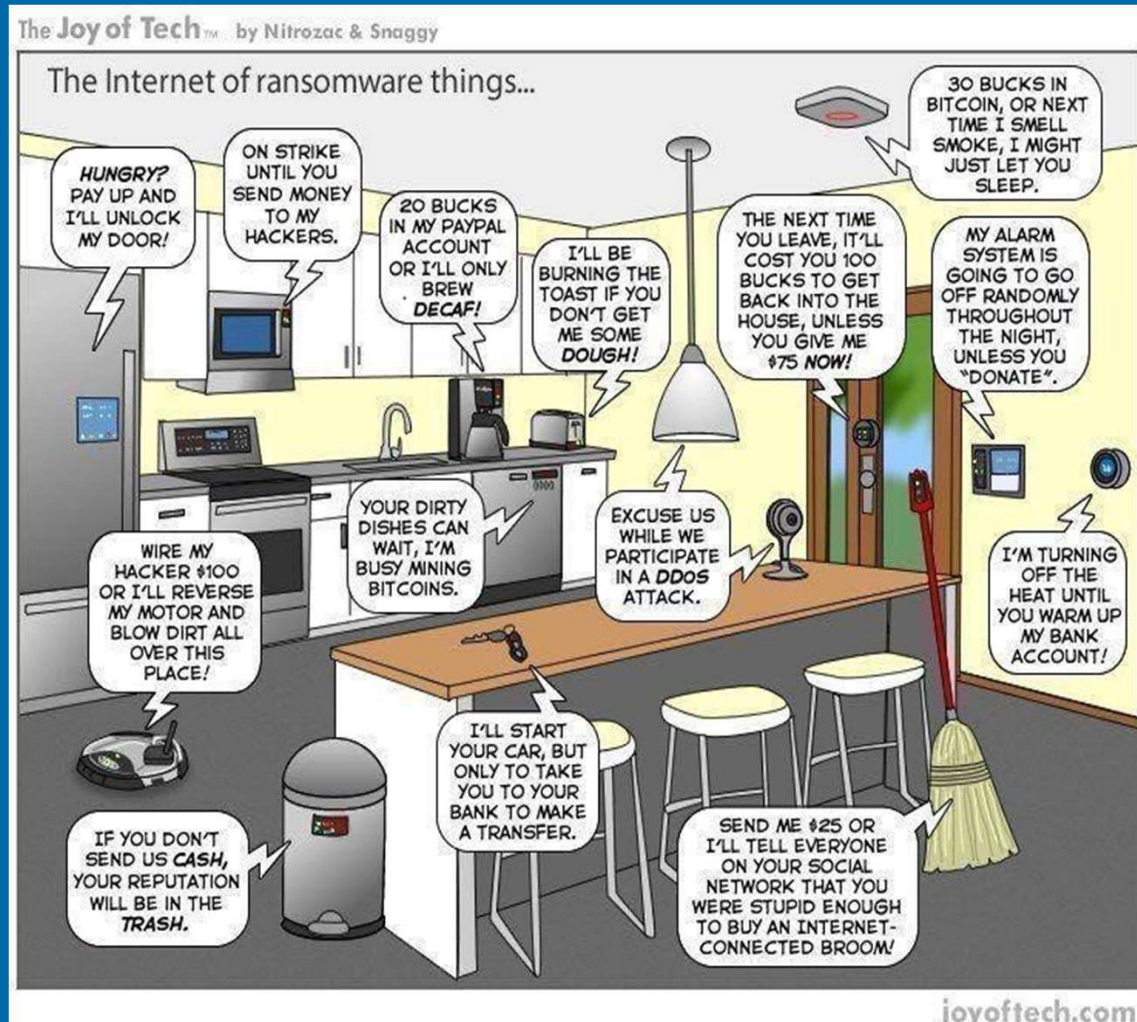
Threats: Social Media

- New channels for attack
- Conduit to deliver malware
- Users freely share information that can be used for hacking and social engineering
- Data loss
- Billions of targets!
- OSINT



Threats: Internet of Things (IoT)

- 2025: 76 billion "smart" devices
- Often not designed with security in mind
- Vector to attack a network
- Can be used to spy on you and your organization
- Can host malware



Threats: Internet of Things (IoT)

The Washington Post
Democracy Dies in Darkness

Innovations How a fish tank helped hack a casino



Pranay Pathole
@PPathole

Tech enthusiasts: My entire house is smart.

Tech workers: The only piece of technology in my house is a printer and I keep a gun next to it so I can shoot it if it makes a noise I don't recognize.

9:51 PM · Apr 12, 2019 · Twitter for iPhone

Threats: Insider Threats

"A malicious insider is an employee or authorized person who uses his data access for harmful, unethical, or illegal activities. Because of the wider access available internally, insiders are often harder to detect and apprehend than external attackers or hackers" — Answers.com



Guiding principals of security

- Impenetrable security is nearly impossible and very expensive
- Focus on risk
- Take a layered approach
- Threats emerge and evolve constantly
- Invite security to the party from the beginning
- Education and awareness are critical
- Maintain a very healthy dose of skepticism/paranoia

Defenses



3 simple steps to remember

- Stop
- Think
- Protect — Be a human firewall

Defenses: Tooling



CryptoPrevent Anti-Malware



datto



CONNECTWISE[®]
Automate

SecurSence[™]

backupify a datto
company

Defenses: Software updates

- Vendors regularly release updates
- Updates may contain productivity and/or security fixes
- ALL devices that contain software should be updated
- Automate this process if you can

Downloads and updates [Get updates](#)

Recent activity

	Lenovo Vantage	App	10.2006.30.0	Modified today
	Windows Camera	App	2020.504.40.0	Modified today
	Movies & TV	App	10.20032.16211.0	Modified yesterday
	Microsoft Sticky Notes	App	3.7.140.0	Modified yesterday
	Skype	App	15.61.87.0	Modified yesterday
	Movie Maker 10 - FREE	App	2.9.73.0	Modified yesterday
	LastPass for Microsoft Edge	App	4.50.1.0	Modified 6/19/2020
	Cortana	App	2.2005.5739.0	Modified 6/19/2020

Windows Update

*Some settings are managed by your organization
[View configured update policies](#)

Looking for info on the latest updates?
[Learn more](#)

You're up to date
Last checked: Today, 12:21 PM

[Check for updates](#)

*Your organization has turned off automatic updates

Pause updates for 7 days
Visit Advanced options to change the pause period

View update history
See updates installed on your device

Advanced options
Additional update controls and settings

Related links
[Check Storage](#)
[OS build info](#)
[Get help](#)
[Give feedback](#)

Lenovo Vantage

LENOVO VANTAGE
ThinkPad T480

[Dashboard](#) [Device](#) [Security](#)

[BACK](#)

System Update

An up-to-date system is a healthy system.

Last updated: 6/19/2020 9:19 AM
Next scheduled update: 6/29/2020 10:39 AM

[CHECK FOR UPDATES](#)

Available updates

These packages include updates that are critical for the correct operation of your computer. Critical updates help keep your computer more secure and reliable and should be installed as they become available. Recommended updates and optional updates help keep your software up to date and your computer running at its best.

[INSTALL ALL UPDATES](#)

About Mozilla Firefox

Firefox Browser

77.0.1 (64-bit) [What's new](#)

Firefox is up to date

Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.

Want to help? [Make a donation](#) or [get involved!](#)

[Licensing Information](#) [End-User Rights](#) [Privacy Policy](#)

Firefox and the Firefox logos are trademarks of the Mozilla Foundation.

Auto update settings

Automatically install updates

Critical Updates

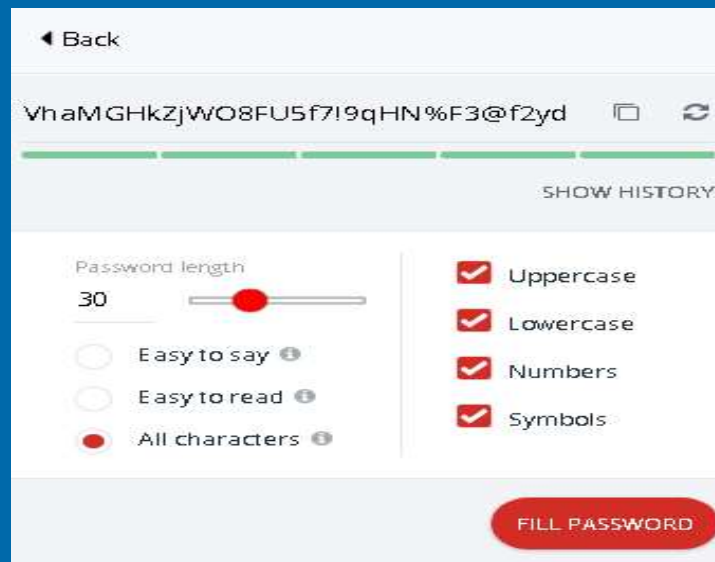
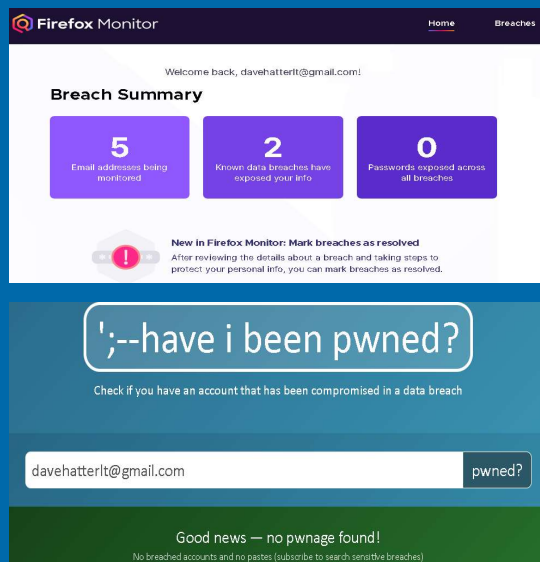
Manage Your Extensions

Enabled

- Cisco Webex Extension
Join Webex meetings using Firefox™
- DuckDuckGo Privacy Essentials
Privacy, simplified. Protect your data as you search and browse; tracker blocking, smarter encl...
- Facebook Container

Defenses: Password Hygiene

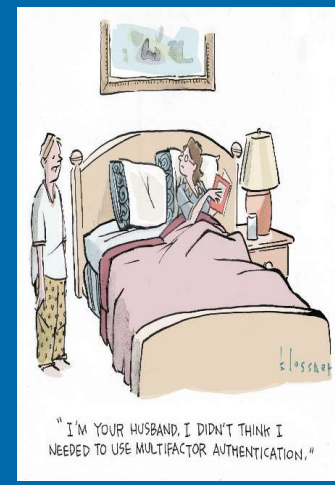
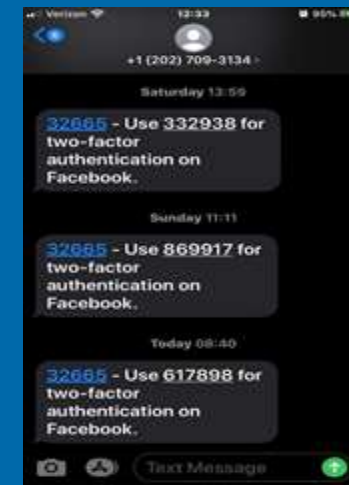
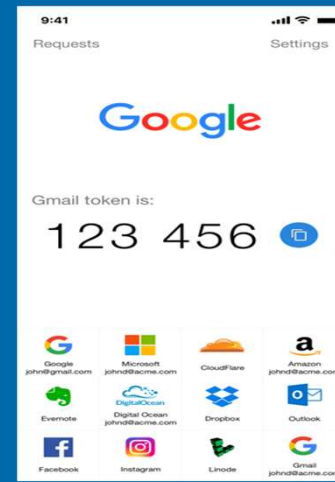
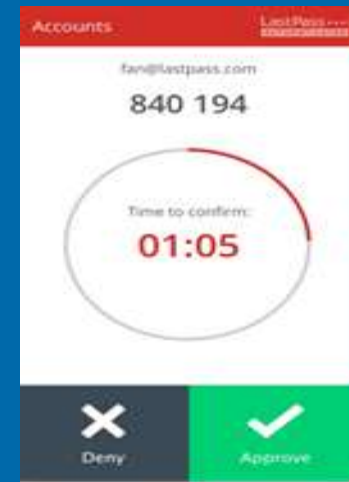
- Use strong, unique passwords for every account
- A passphrase is better. e.g. "1 l0ve pizz@ with 0ni0ns"
- Use a password manager with MFA.
- Check the Dark Web for leaked creds



- ❌ Previous breach exposures
- ❌ Less than 8 characters
- ❌ Context-specific words
- ❌ Dictionary words
- ❌ Repetitive characters
- ❌ Password hints

Defenses: Multi-factor Authentication

- MFA: aka Two-factor Authentication (2FA) or Two-Step Verification
- Microsoft and Google have recently indicated MFA can stop 99% of all automated attacks
- Enable MFA everywhere
- Use an authenticator app or hardware key rather than SMS based OTPs



Defenses: Endpoint Protection

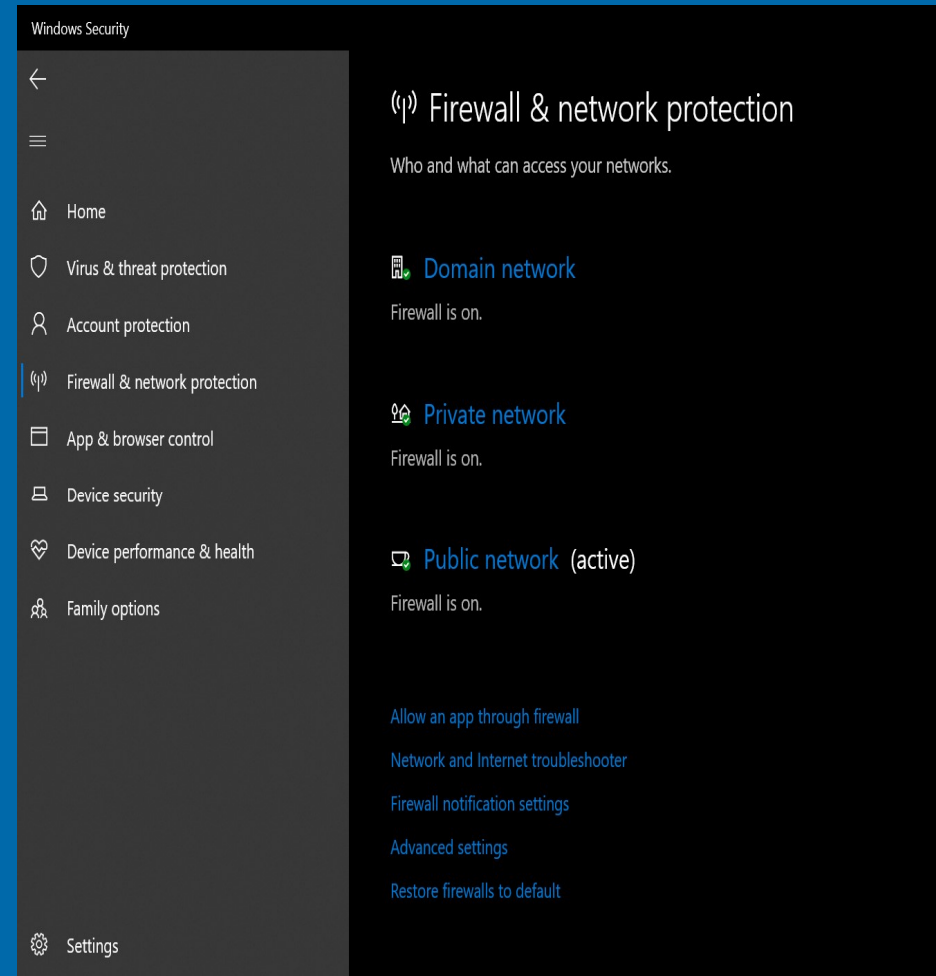
- Vendors regularly release updates
- Also known as anti-malware or anti-virus software
- Update definitions
- Disable everything and enable functionality as required
- Consider more than one



Source: Gartner (May 2021)

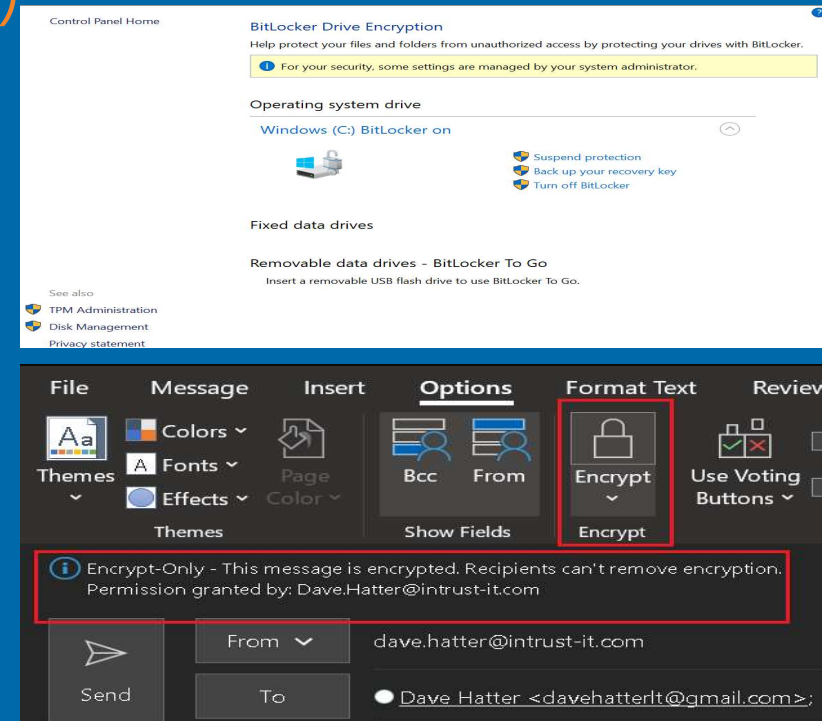
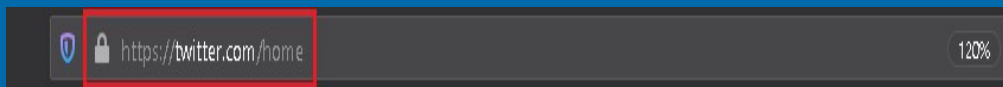
Defenses: Firewall

- Use a firewall to protect your device / network
- Your router can be configured to be a firewall
- Windows comes with a software firewall



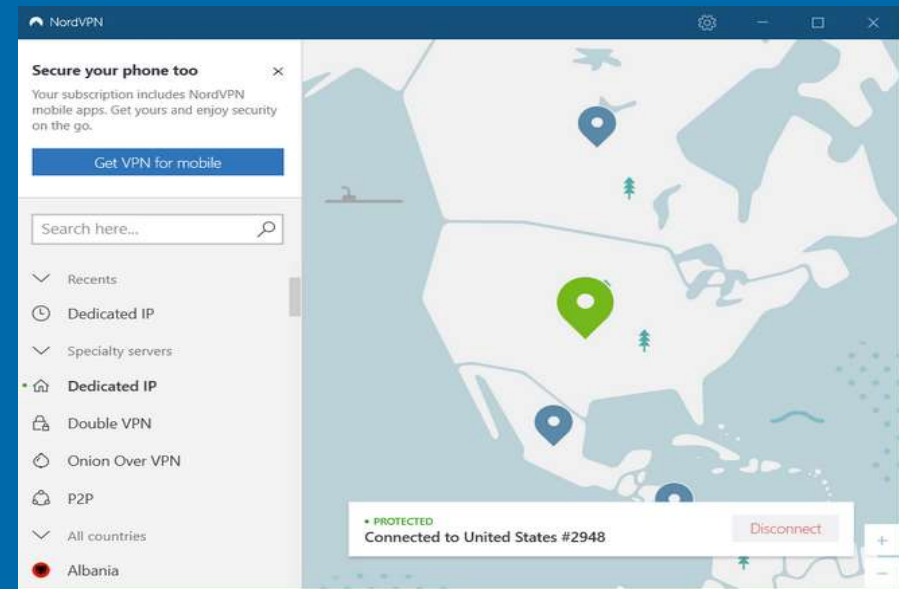
Defenses: Encryption

- Encryption scrambles data so that it can only be unscrambled with the appropriate key
- Use Encryption (at rest and in motion)
- Enable BitLocker for data at rest
- Look for https:// in the browser
- Use encryption to protect email
- Use encryption to protect messaging



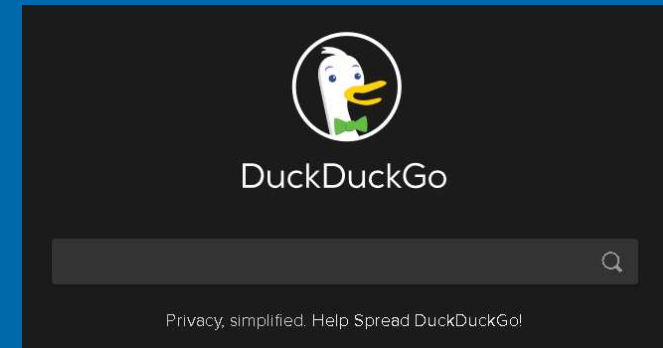
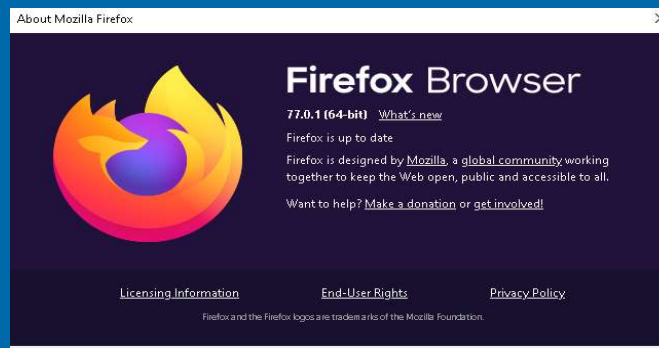
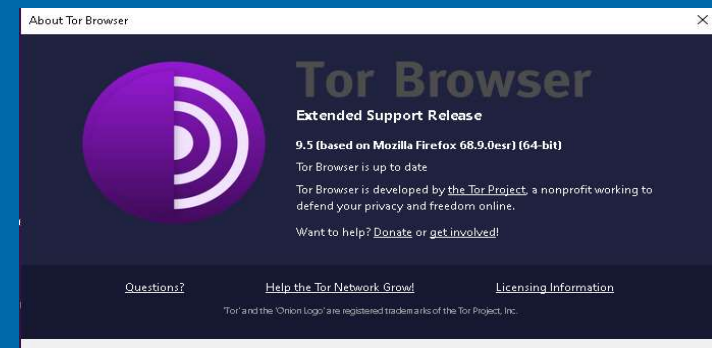
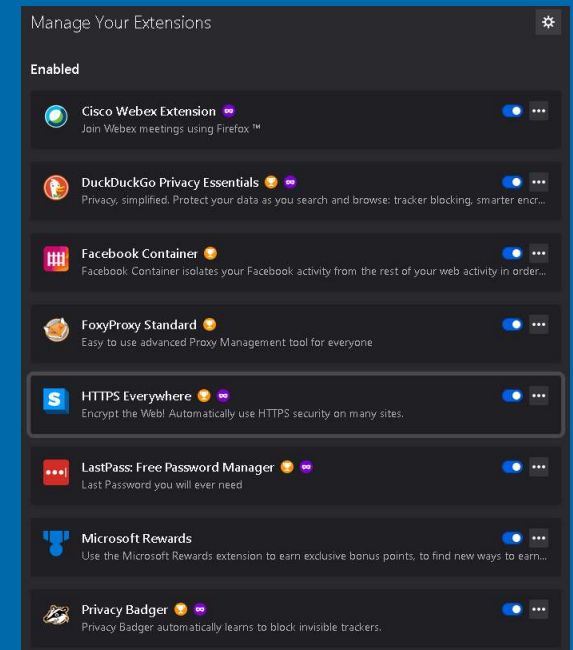
Defenses: Virtual Private Network

- A VPN creates an encrypted connection
- May not be required if all your apps are cloud based
- Never use public Wi-Fi without a VPN
- The best include NordVPN, IPVanish and TunnelBear
- Vet the VPN software carefully!



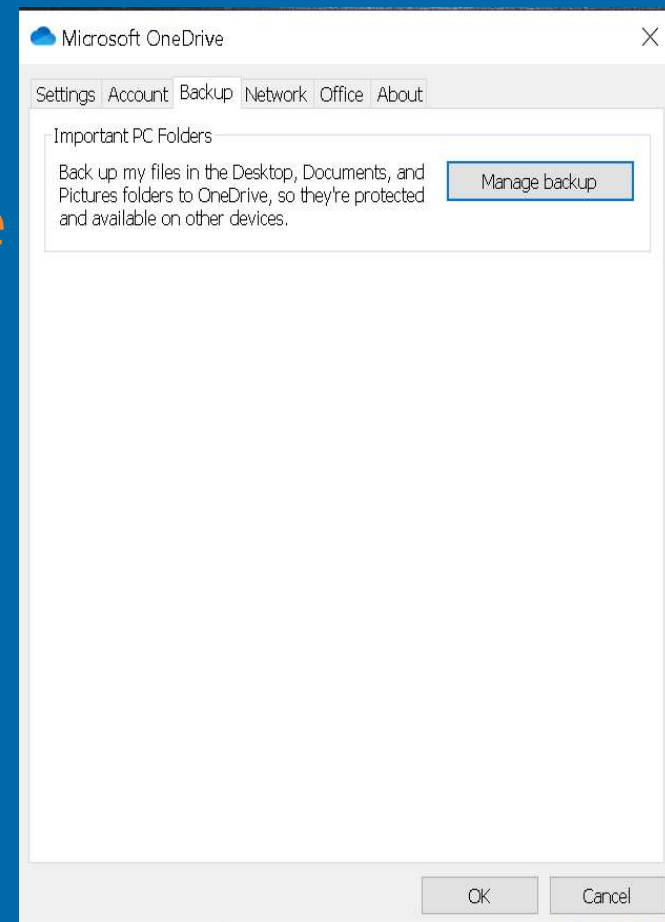
Defenses: Vet software carefully

- Do your homework and vet apps
- Don't download the latest viral thing
- This applies to desktop apps, mobile apps, and browser extensions
- Delete apps you don't need
- Use privacy friendly platforms & apps



Defenses: Backup

- Backup data and verify the backup integrity
- 3-2-1 rule: At least three versions of your data on two different media, one of which is off-site
- Look for a service that allows you to define a personal encryption key. If not, read the privacy policy carefully
- Tools like OneDrive can be a basic backup
- iDrive and BackBlaze rate highly
- We love Datto



Defenses: Network

- Change default password to a strong password
- Enable WPA2 or higher encryption
- Enable firewall
- Update regularly
- Use a guest network

Security Options

- ☐ None
- ☒ WPA2-PSK [AES]
- ☐ WPA-PSK [TKIP] + WPA2-PSK [AES]
- ☐ WPA/WPA2 Enterprise

Router Auto Firmware Update

Enable router to automatically update to future firmware. This keeps your router up to date with the latest features and security fixes. Select one of the following options:

- ☒ Enable
- ☐ Disable

Firmware Version Check

No new firmware version available.

OK

Defenses: Hardening

- Configuring systems to make them more difficult to hack
- For example, change default passwords and remove unnecessary accounts
- Lock the screen when not in use
- Don't make work devices visible on the network
- Check out the CIS Benchmarks



The screenshot shows the CIS Benchmarks website. At the top, there's a navigation bar with "Home" and "CIS Benchmarks". Below this is the CIS Benchmarks logo, which consists of a blue circle with a white 'B' inside, followed by the text "CIS Benchmarks™". To the right of the logo is a large image of people working at computers in an office setting. Below the logo, there's a video player showing a man speaking, with a play button overlay. To the right of the video player, there's a text block that reads: "With our global community of cybersecurity experts, we've developed CIS Benchmarks: 140+ configuration guidelines for various technology groups to safeguard systems against today's evolving cyber threats." At the bottom of the page, there are three main sections: "Overview of CIS Benchmarks and CIS-CAT Demo", "Register for the Webinar" (with dates: Tues. June 23 at 10:00 AM EDT and Tues. July 7 at 1:30 PM EDT), and "CIS Benchmarks FAQ". On the far right, there's a green button that says "Access all Benchmarks →".

Defenses: Use a framework

- NIST published first version of the Cybersecurity Framework (CSF) in February 2014
- CSF maps to multiple frameworks such as ISO 27001, CIS Controls & more
- Version 1.1 was published in April 2018
- We love the CIS Controls V8

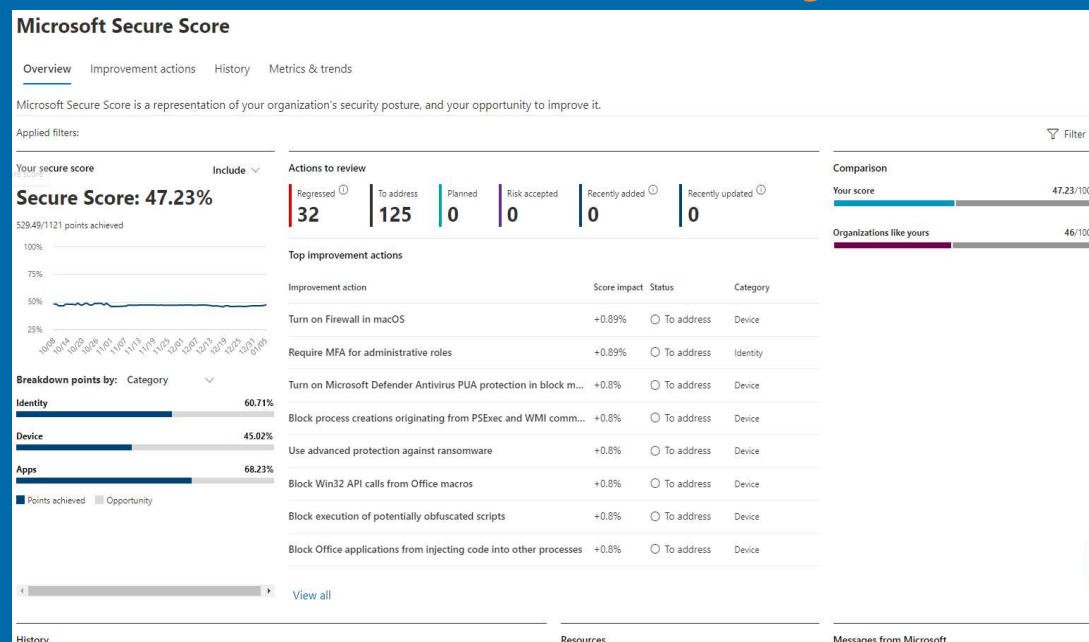
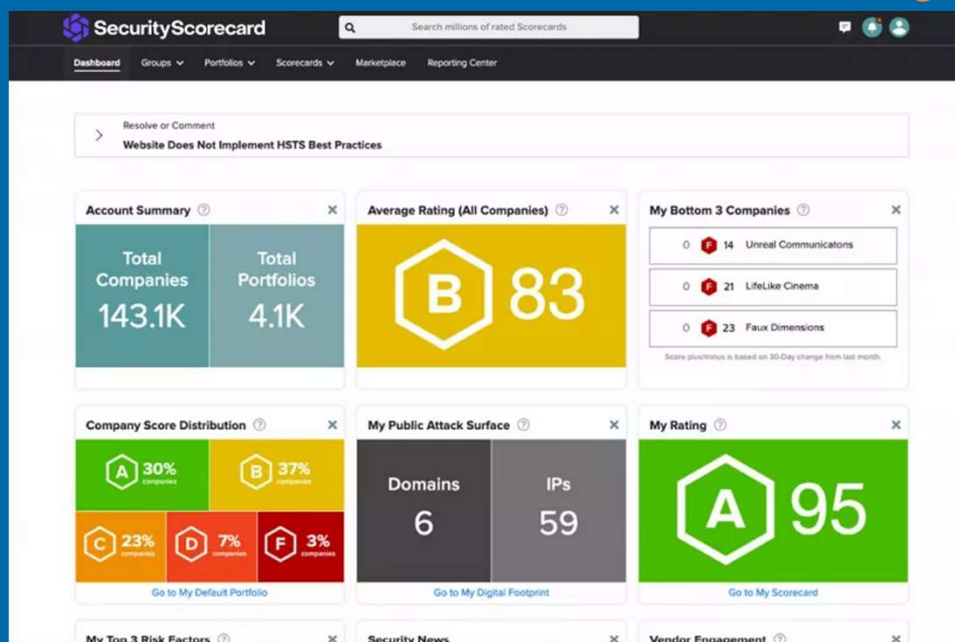


CIS Controls Version 8

Defenses: Secure Bank Accounts

- Setup controls and limits on ACH and wire-transfers for your business account
- Consider paper check positive pay, or use a separate account to write checks out of
- Talk to your bank about available protections

Defenses: Security Posture Visibility



Defenses: New clients

- Always vet new business leads by going to the potential customer's website and verifying contact information
- Avoid business deals done strictly via email
- Be cautious about how and when you give out key information
- Be wary of email communication done strictly via generic email accounts
- Be suspicious of email domains that don't match the company's website or end in alternates like .net, .info, .us, etc
- Understand that anything can be spoofed
- Trust AND verify

Defenses: Limit digital footprint

- Delete old unused email accounts and/or old emails
- Delete old content from social media platforms
- Disconnect apps and platforms to stop information leakage
- Lock down social media and understand the privacy settings
- Use a Virtual Private network (VPN)
- Use privacy friendly platforms and tools:
 - DuckDuckGo (search)
 - Tor
 - Firefox
 - Brave
- Lock down your browser and use extensions to limit tracking

Defenses: Limit digital footprint

- Create "burner" accounts
- Turn off services like location and Bluetooth when not needed
- Ensure that cloud-based backups are secured with a password, MFA where possible, and encrypted
- Do Dark Web searches for leaked data
- Use Google Alerts to find information online
- Work with a company like Delete Me who for a fee will provide annual "protection plans" that guarantee removal of your personal data from data-broker services
- Understand that old content may be archived somewhere like the Wayback Machine: <https://archive.org/web/web.php>

Defenses: Cloud Services

- Cloud based services offer advanced security and backup capability
 - Microsoft 365 / Azure
 - G Suite

Defenses: General

- Prioritize risk
- Be wary of remote access
- Sanitize old equipment
- Maintain a clean desk policy
- Vendor management
- Disable devices that can watch/listen while working
- Don't allow family to use work devices
- Keep work data on work devices only

Defenses: General

- Use secure videoconferencing
- Be careful about information you share
- Shred work-related documents
- Get cyberinsurance, read policy carefully
- Create policies and procedures
- Have an incident response plan
- Engage early and often with your security team
- SETA (Security, Education, Training and Awareness)

Be vigilant and keep learning!

**YOU SAY INFORMATION SECURITY
IS IMPORTANT BUT YOU AVOID
AWARENESS TRAINING**



**BUT THAT'S NONE OF MY
BUSINESS**

Hope and denial are NOT a strategy!

Remember the 3 simple steps

- Stop
- Think
- Protect – Be a human firewall

Skepticism and Security

FRANK'S
RedHot



I put that  on everything™

Cybersecurity myths dispelled

- My organization is too small or insignificant to be a target
- My data (or the data I have access to) isn't valuable
- Attacks are always sophisticated or technically complex
- New software and devices are secure out-of-the-box
- Cybersecurity is an IT issue

For more information follow:

- Bruce Schneier: @schneierblog
- Kevin Mitnick: @kevinmitnick
- US-CERT: @USCERT_gov
- SecurityWeek: @SecurityWeek
- Center for Internet Security: @CISecurity
- MSRC: @msftsecresponse
- NIST Cyber: @NISTcyber
- Intrust IT: @IntrustIT
- MSRC: @msftsecresponse
- Microsoft Secure: @msftsecurity
- RSA: @RSAsecurity
- Mikko Hypponen: @mikko
- Troy Hunt: @troyhunt
- CSOnline: @CSOonline
- Me: @DaveHatter

Additional Resources

- www.intrust-it.com/outsourcing-your-worry
- www.twofactorauth.org
- www.safer-networking.org
- www.webopedia.com
- www.opendns.com
- www.hackerwatch.org
- www.haveibeenpwned.com
- www.twofactorauth.org
- www.knowbe4.com
- www.antiphishing.org
- www.microsoft.com/security
- www.idtheftcenter.org/facts.shtml
- www.ic3.gov/default.aspx
- www.securityscorecard.com
- www.datto.com
- www.sentinelone.com
- www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm
- enterprise.verizon.com/resources/reports/dbir/
- www.us-cert.gov/ncas/current-activity/2019/11/06/cisa-launches-cyber-essentials-small-businesses-and-small-slts
- www.nist.gov/cyberframework
- www.cisecurity.org
- www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- www.pcmag.com/roundup/256703/the-best-antivirus-protection
- www.knowbe4.com/ransomware-simulator
- www.zdnet.com
- www.cnet.com
- www.cisa.gov
- docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls
- www.youtube.com/c/KitbogaShow

Q & A



"You are an essential ingredient in our ongoing effort to reduce Security Risk."- Kirsten Manthorne



THANK YOU!

Dave Hatter, CISSP, CCSP, CCSLP, Security +, Network+, PMP, PMI-ACP, ITIL V3

Intrust IT

[linkedin.com/in/davehatter](https://www.linkedin.com/in/davehatter)

twitter.com/davehatter

www.youtube.com/user/davidlhatter

Listen to Tech Friday live on 55KRC at 6:30 AM every Friday on 550 AM or
<http://www.55krc.com>

Watch Cyber Monday live on WTVG at 6:30 AM every Monday on 13 ABC or
<https://www.13abc.com/>