intrust IT

CYBERSECURITY

NOT JUST FOR IT ANYMORE

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

Cyber Security Consultant

Intrust IT

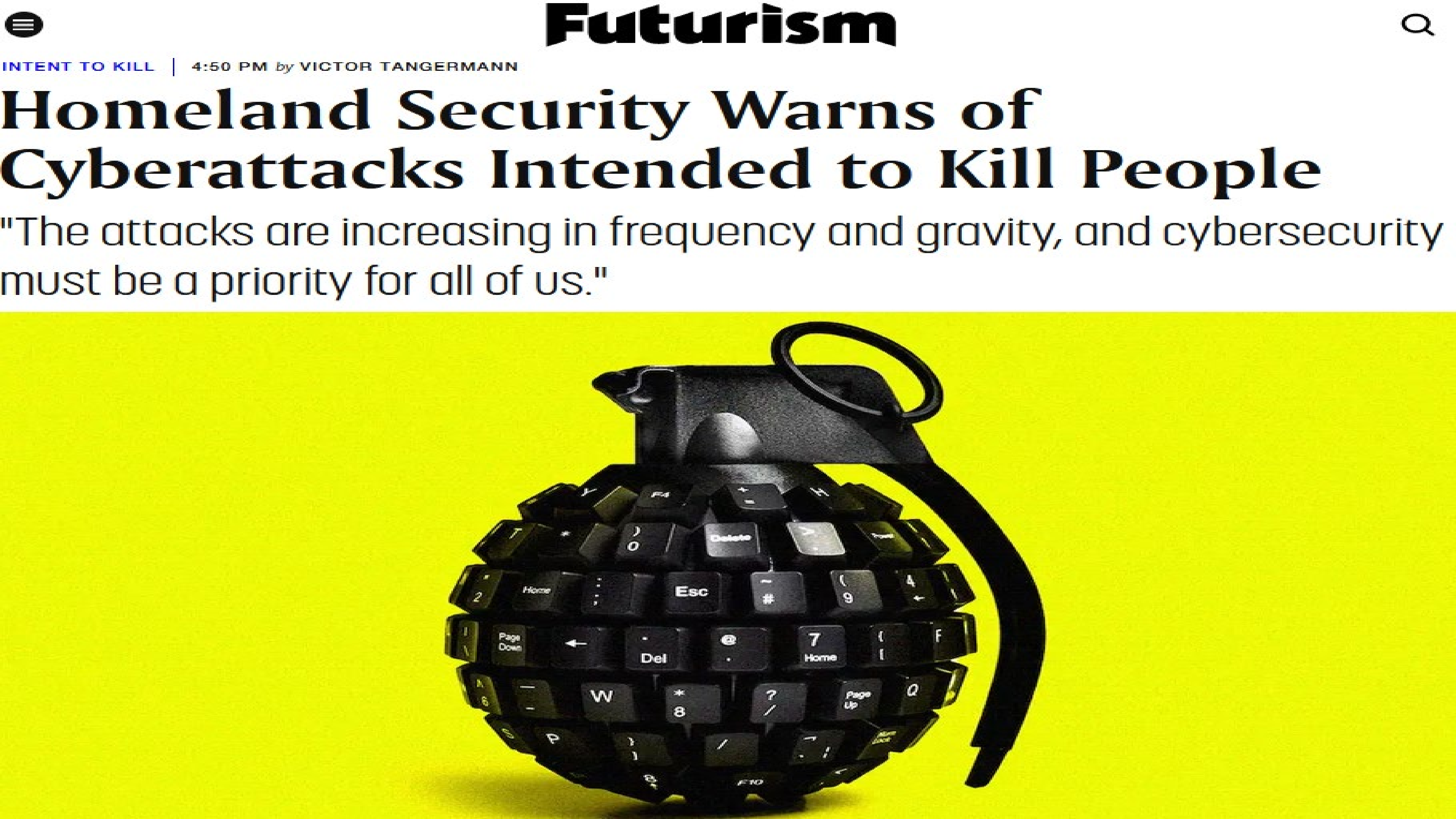
linkedin.com/in/davehatter

twitter.com/davehatter

www.youtube.com/user/davidlhatter

My goals for today

- Educate you
- Motivate you
- Provide actionable advice
- Have fun



Futurism

INTENT TO KILL | 4:50 PM *by* VICTOR TANGERMANN

Homeland Security Warns of Cyberattacks Intended to Kill People

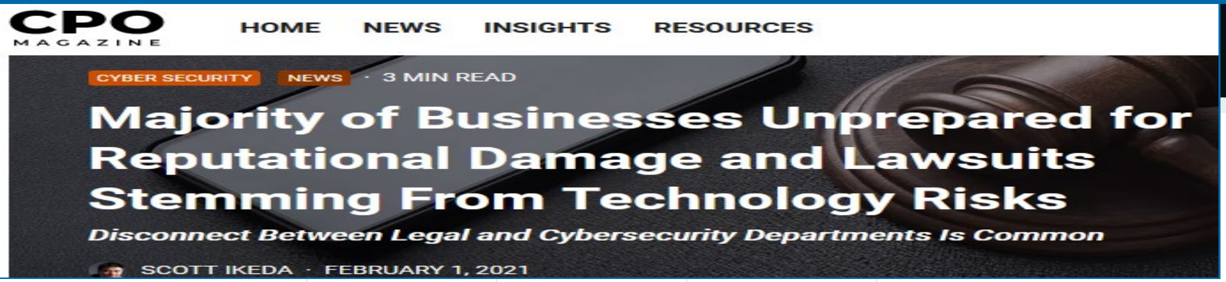
"The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us."

- Defense in Depth
- Patched systems
- 24/7 monitoring/ alerting
- Annual compliance auditing
- Experienced IT/ Security team
User clicks on an email
made with mematic

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
- Cybersecurity requires a huge financial investment
- Cyber breaches are covered by general liability insurance
- Security is an IT issue

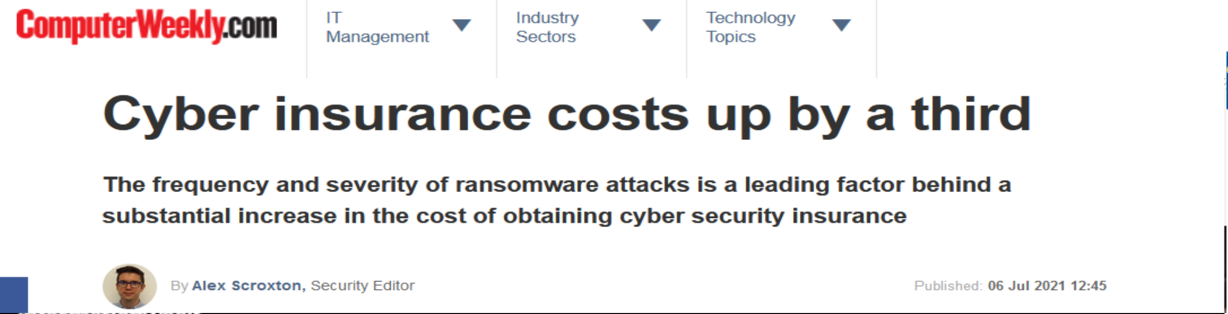
Ripped from the headlines…



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

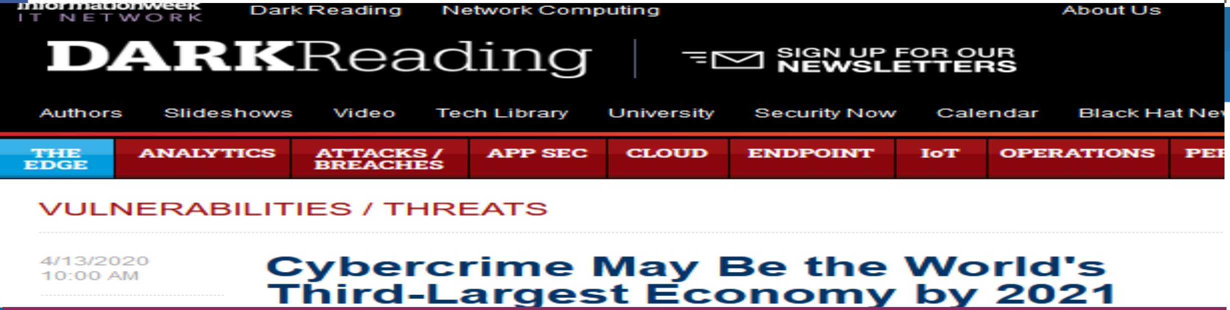


Cyber insurance costs up by a third

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

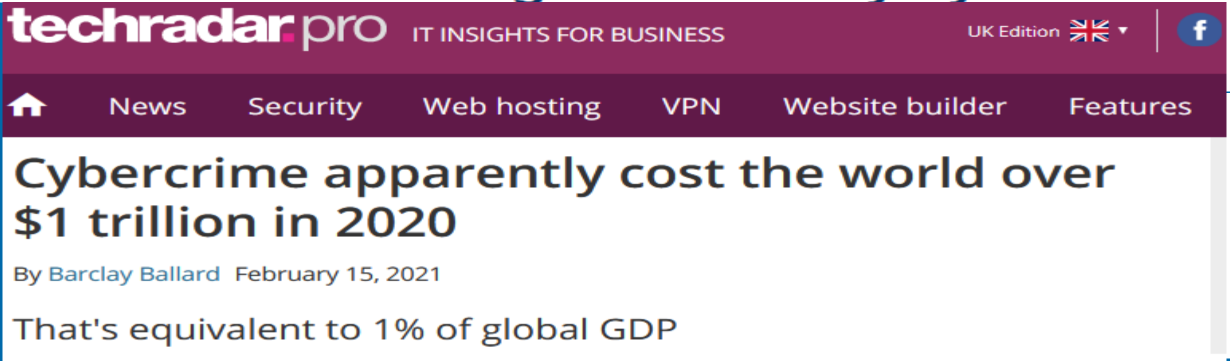
Published: 06 Jul 2021 12:45



VULNERABILITIES / THREATS

4/13/2020 10:00 AM

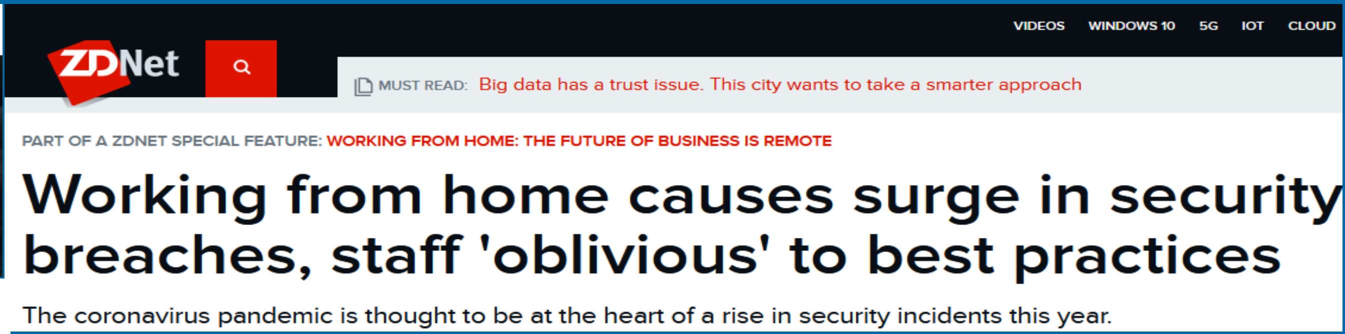
Cybercrime May Be the World's Third-Largest Economy by 2021



Cybercrime apparently cost the world over $1 trillion in 2020

By Barclay Ballard February 15, 2021

That's equivalent to 1% of global GDP

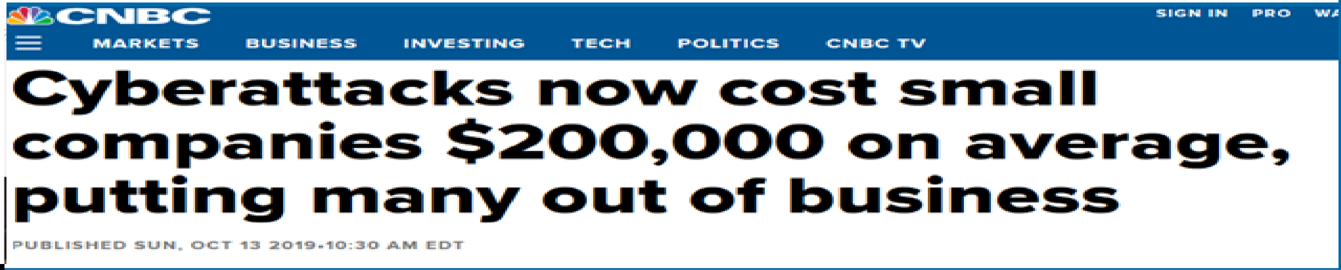


MUST READ: Big data has a trust issue. This city wants to take a smarter approach

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

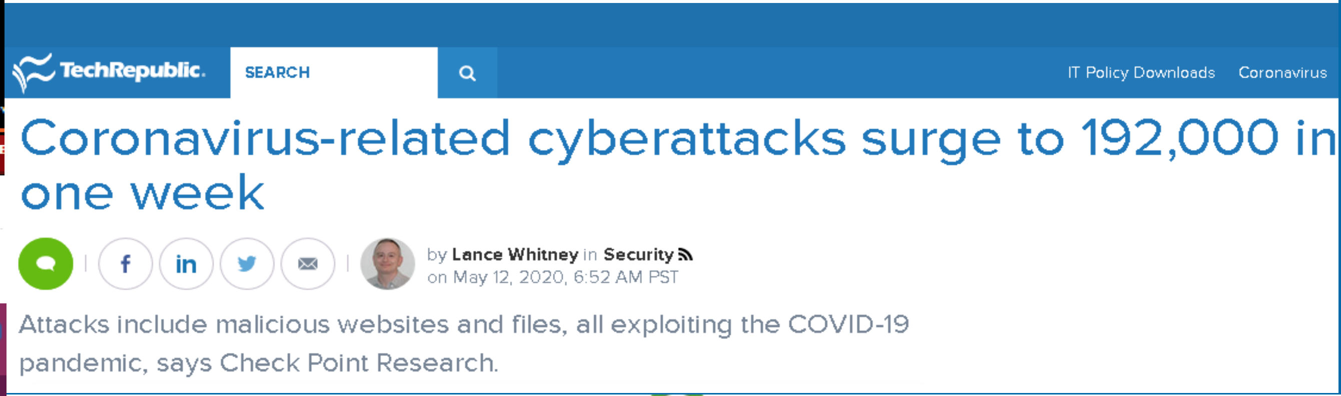
Working from home causes surge in security breaches, staff 'oblivious' to best practices

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



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

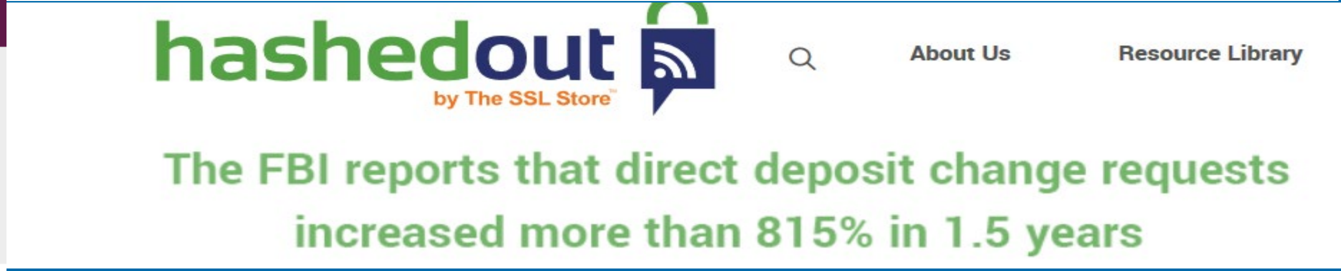
PUBLISHED SUN, OCT 13 2019•10:30 AM EDT



Coronavirus-related cyberattacks surge to 192,000 in one week

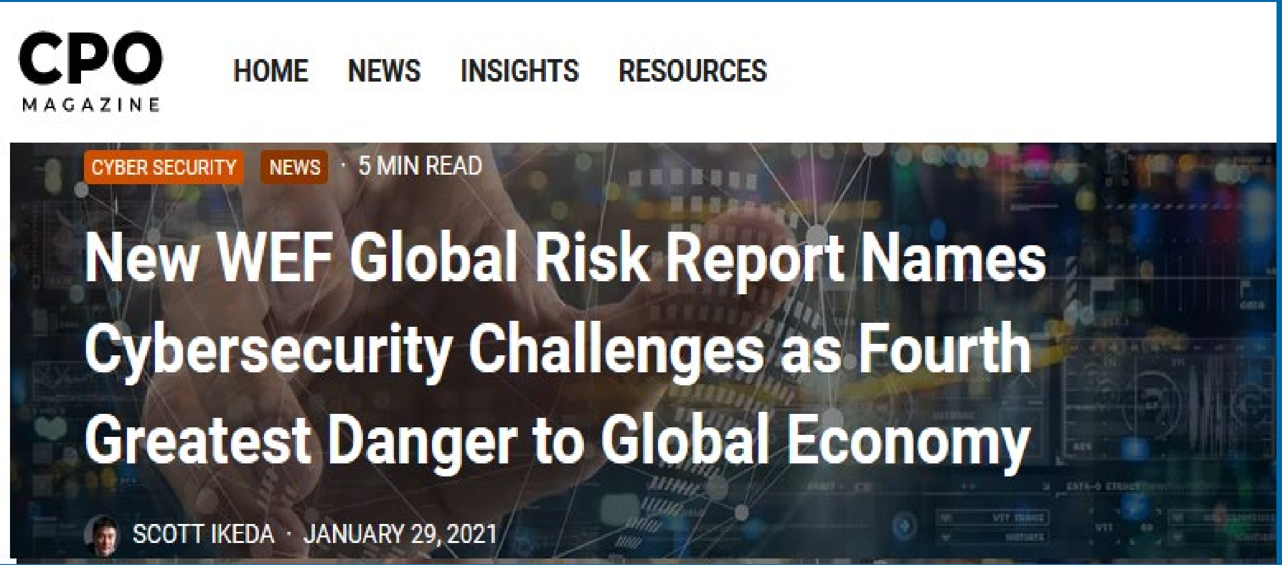
by Lance Whitney in Security on May 12, 2020, 6:52 AM PST

Attacks include malicious websites and files, all exploiting the COVID-19 pandemic, says Check Point Research.



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

Ripped from the headlines…



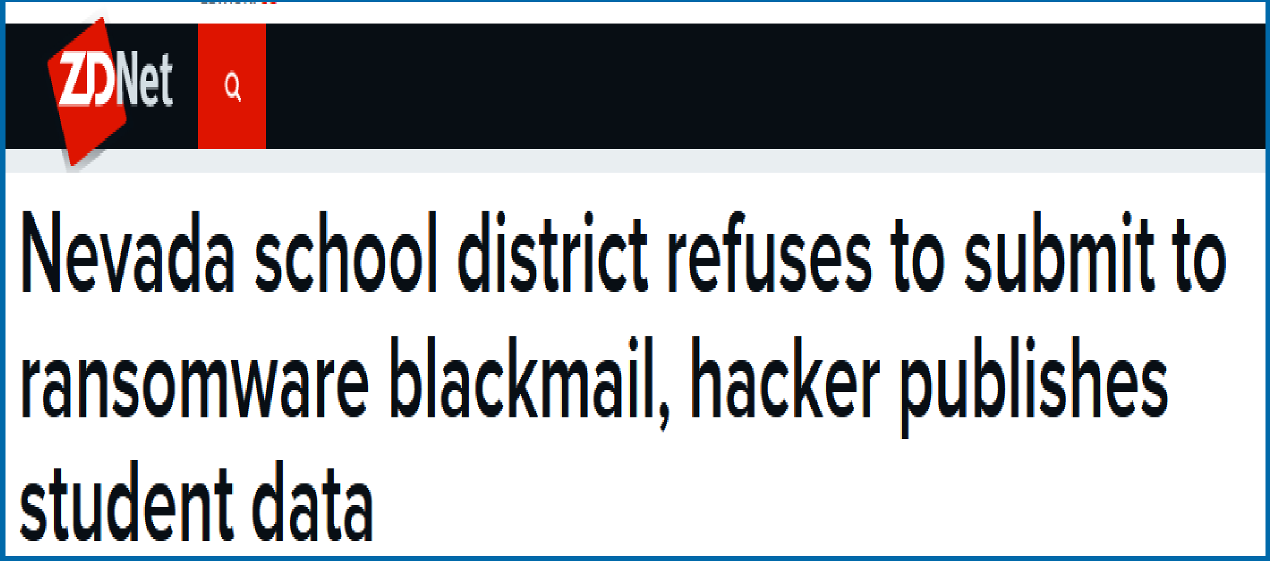
CPO MAGAZINE

HOME NEWS INSIGHTS RESOURCES

CYBER SECURITY · NEWS · 5 MIN READ

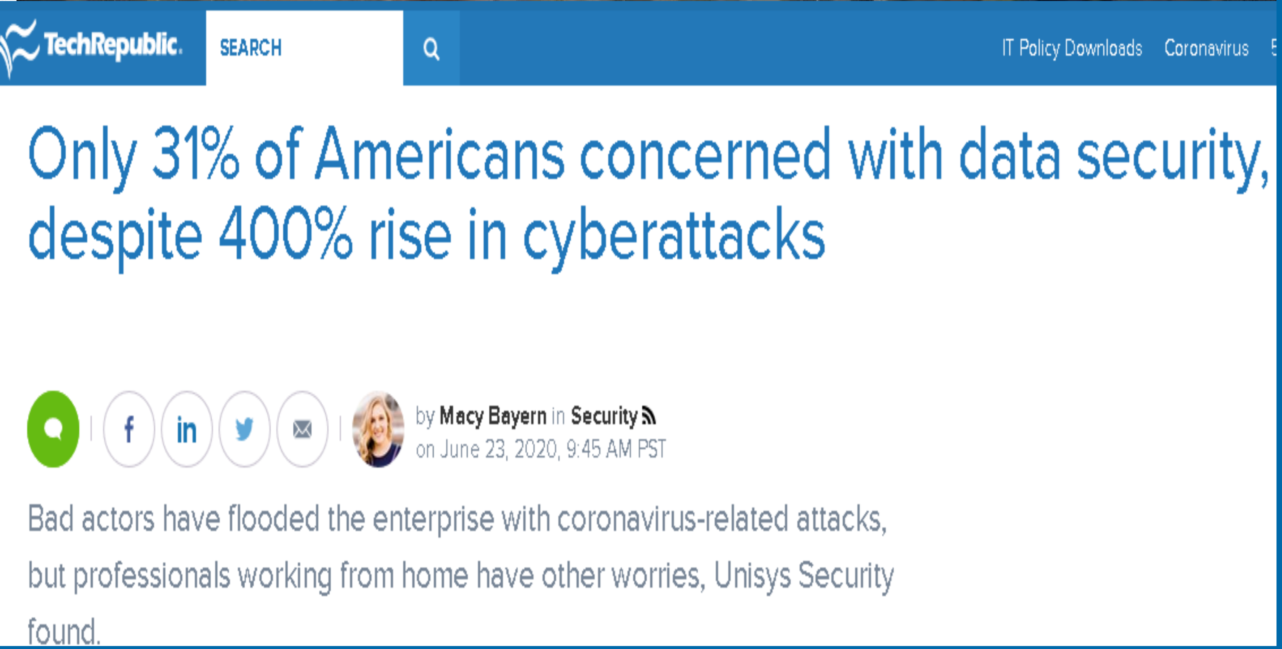
New WEF Global Risk Report Names Cybersecurity Challenges as Fourth Greatest Danger to Global Economy

SCOTT IKEDA · JANUARY 29, 2021



ZDNet

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



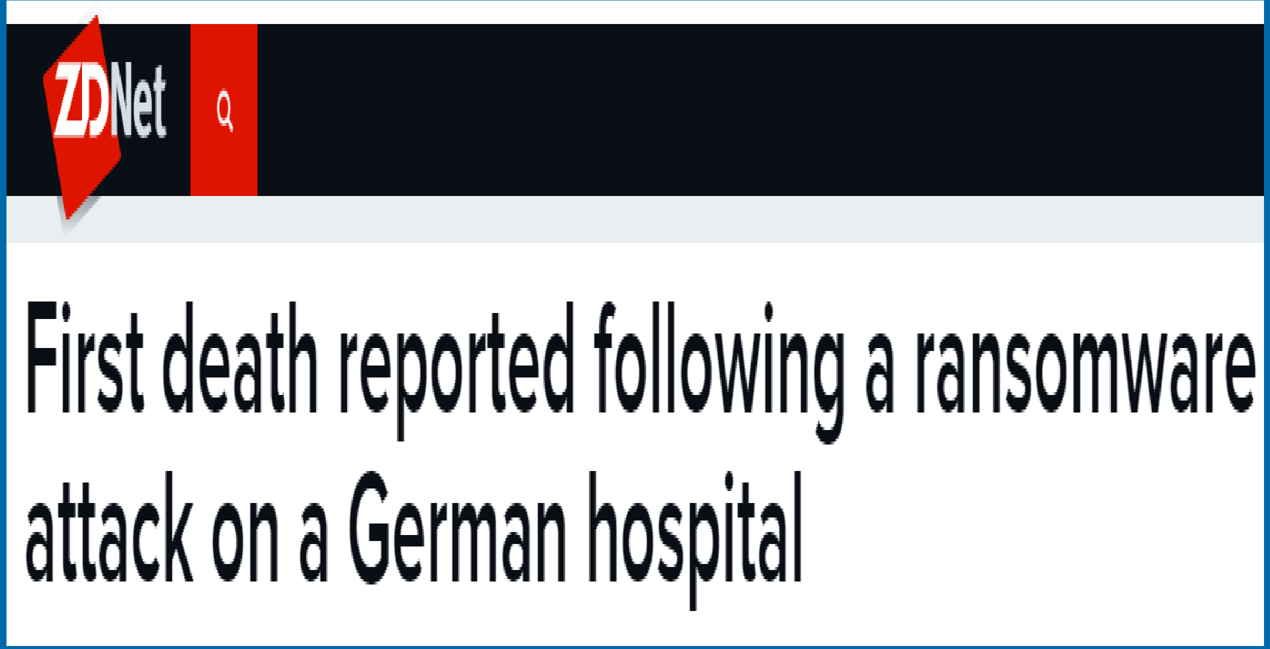
TechRepublic. SEARCH

IT Policy Downloads Coronavirus 5

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

First death reported following a ransomware attack on a German hospital

Something to consider...

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." - Stephane Nappo

Technology impacts all organizations

- Technology is increasingly important to organizations of all shapes and sizes
- Projects increasingly implement new technology
- Technology is increasingly used to manage projects
- Gartner forecasts 2021 IT spending to be $4 trillion

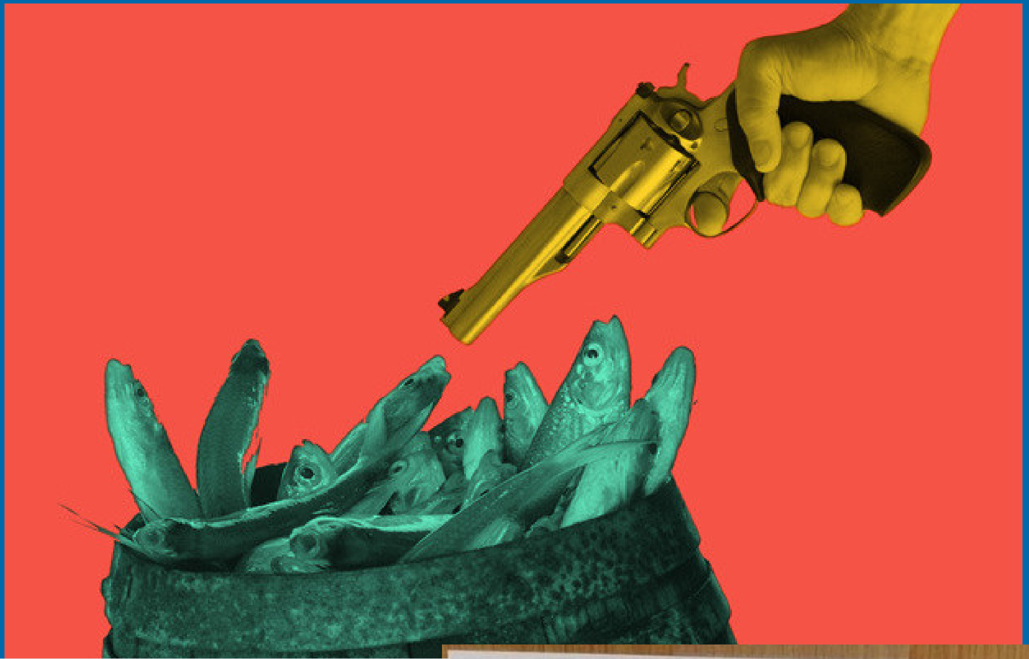
It’s a matter of when, not if…

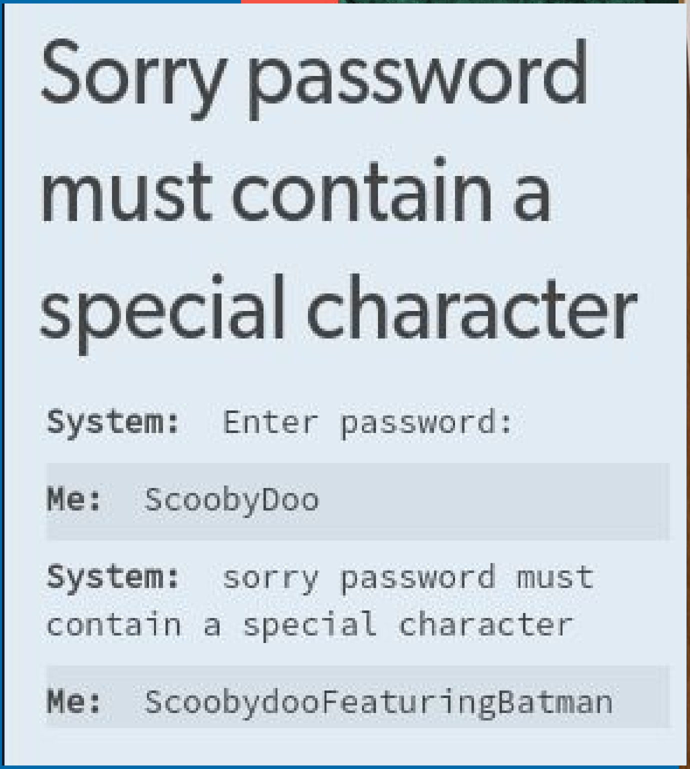
- “No locale, no industry or organization is bulletproof when it comes to the compromise of data.” – Verizon 2016 Data Breach Investigation Report
- “However terrified you are about cybersecurity, you’re probably not terrified enough.” – LinkedIn Co-founder Reid Hoffman
- Cybercrime is “the greatest 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

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.”

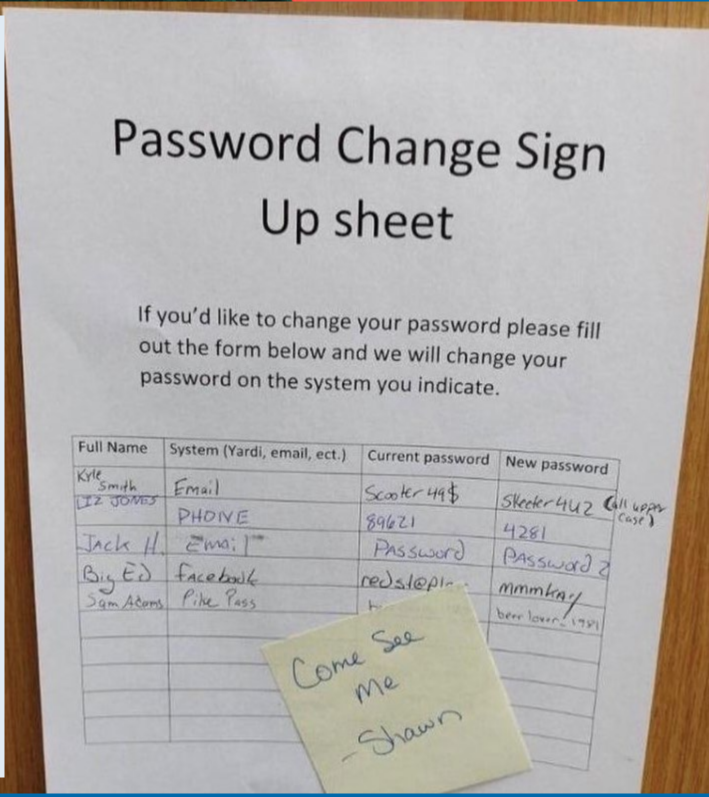
https://www.csoonline.com/article/2866911/why-criminals-pick-on-small-business.html





Sorry password must contain a special character

```
System:  Enter password:
Me:  ScoobyDoo
System:  sorry password must
contain a special character
Me:  ScoobydooFeaturingBatman
```



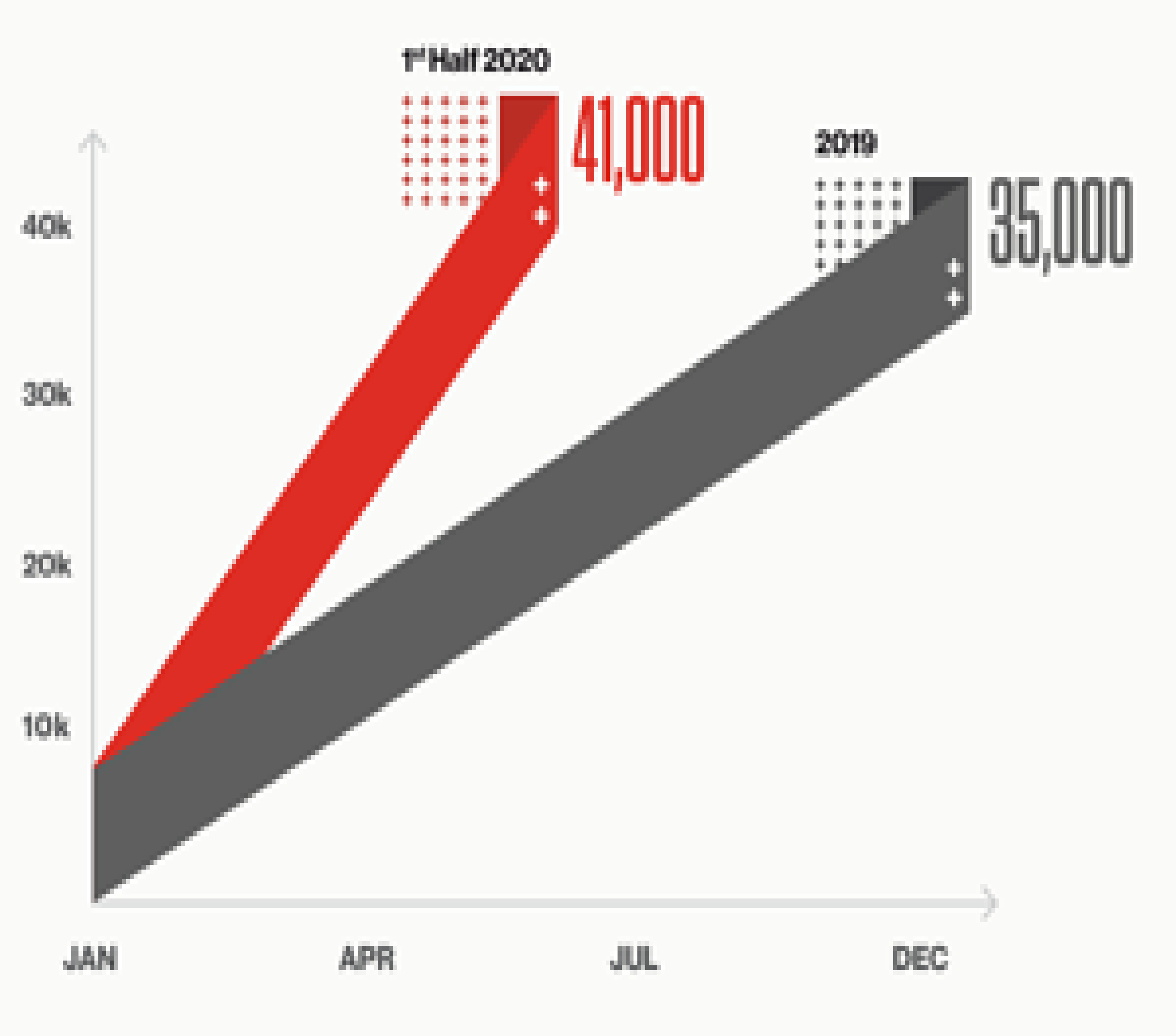
Password Change Sign Up sheet

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	Scooter49$	Skeeter442 (all upper case)
~~LIZ JONES~~	PHONE	89621	4281
Jack H.	Email	Password	Password2
Big ED	facebook	redsl@pl	mmmkay
Sam Adams	Pike Pass	h	beer lover 1981

Come See Me
-Shawn

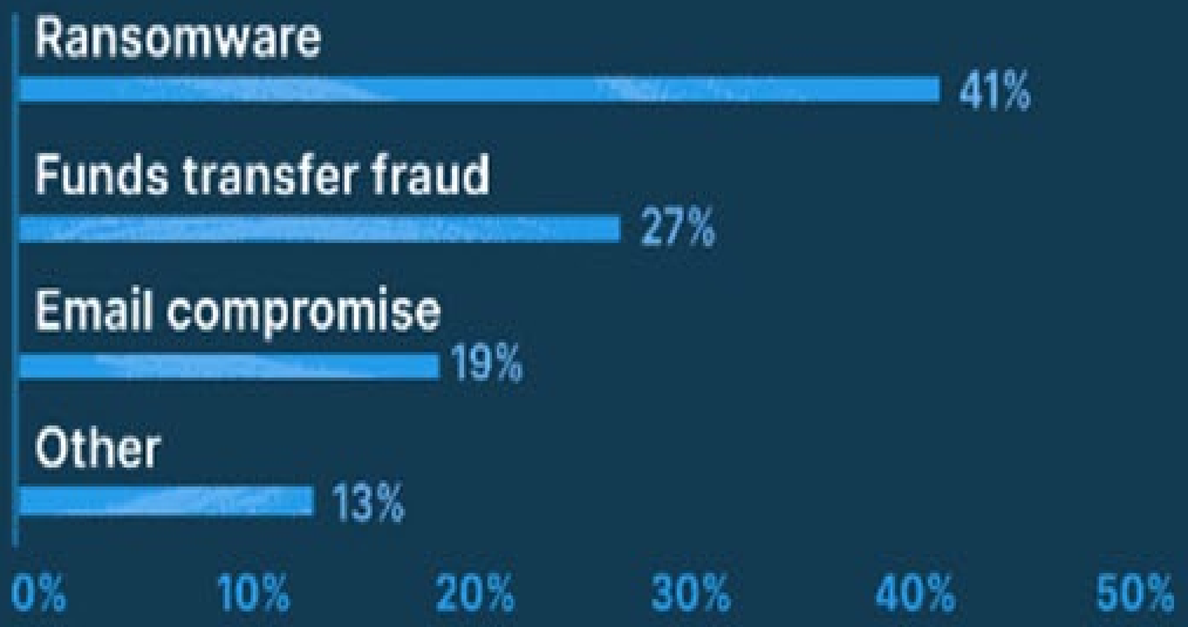
By the numbers…



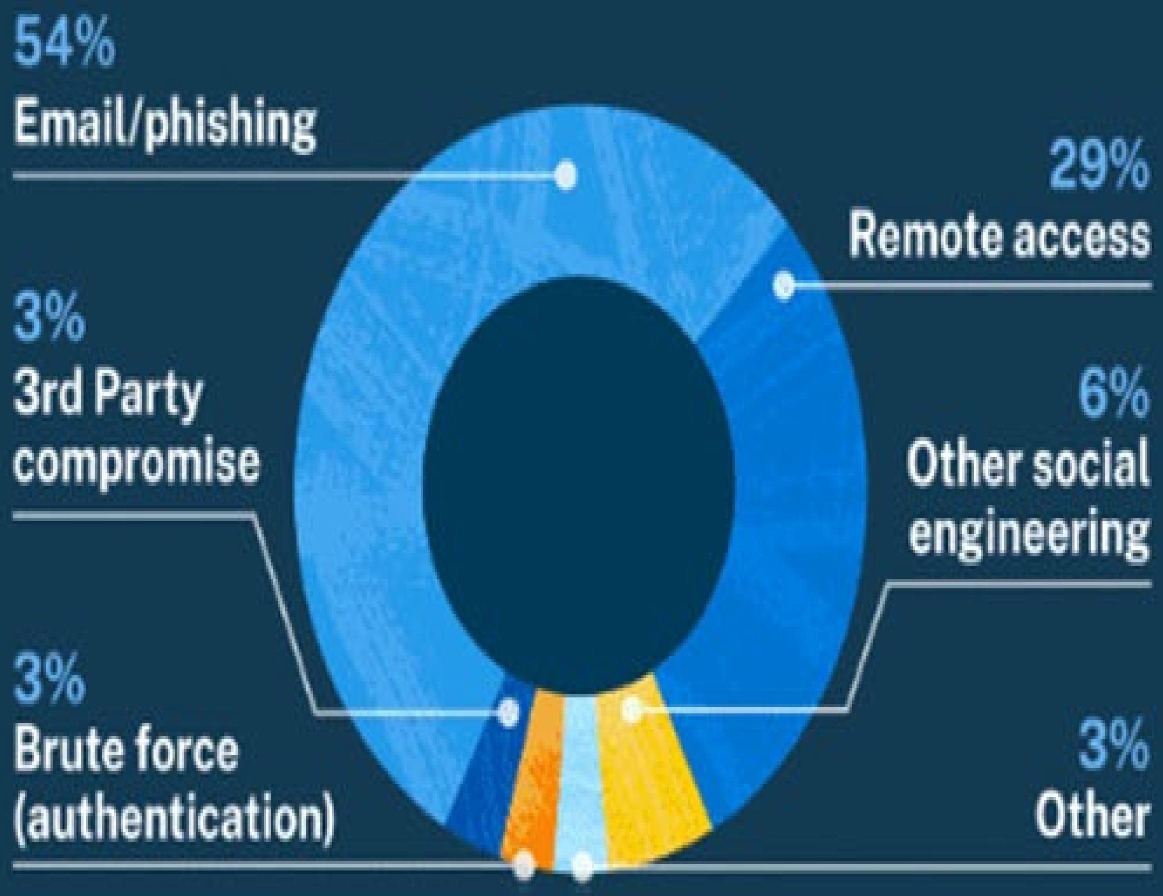
- CrowdStrike, reported detecting and blocking roughly 41,000 potential intrusions in the first half of 2020
- Up from 35,000 intrusions over 12 months in 2019
- This is a 154% increase in cyberattacks

By the numbers…

Most common cyber incidents (% of reported claims)



Percentage of claims by attack technique

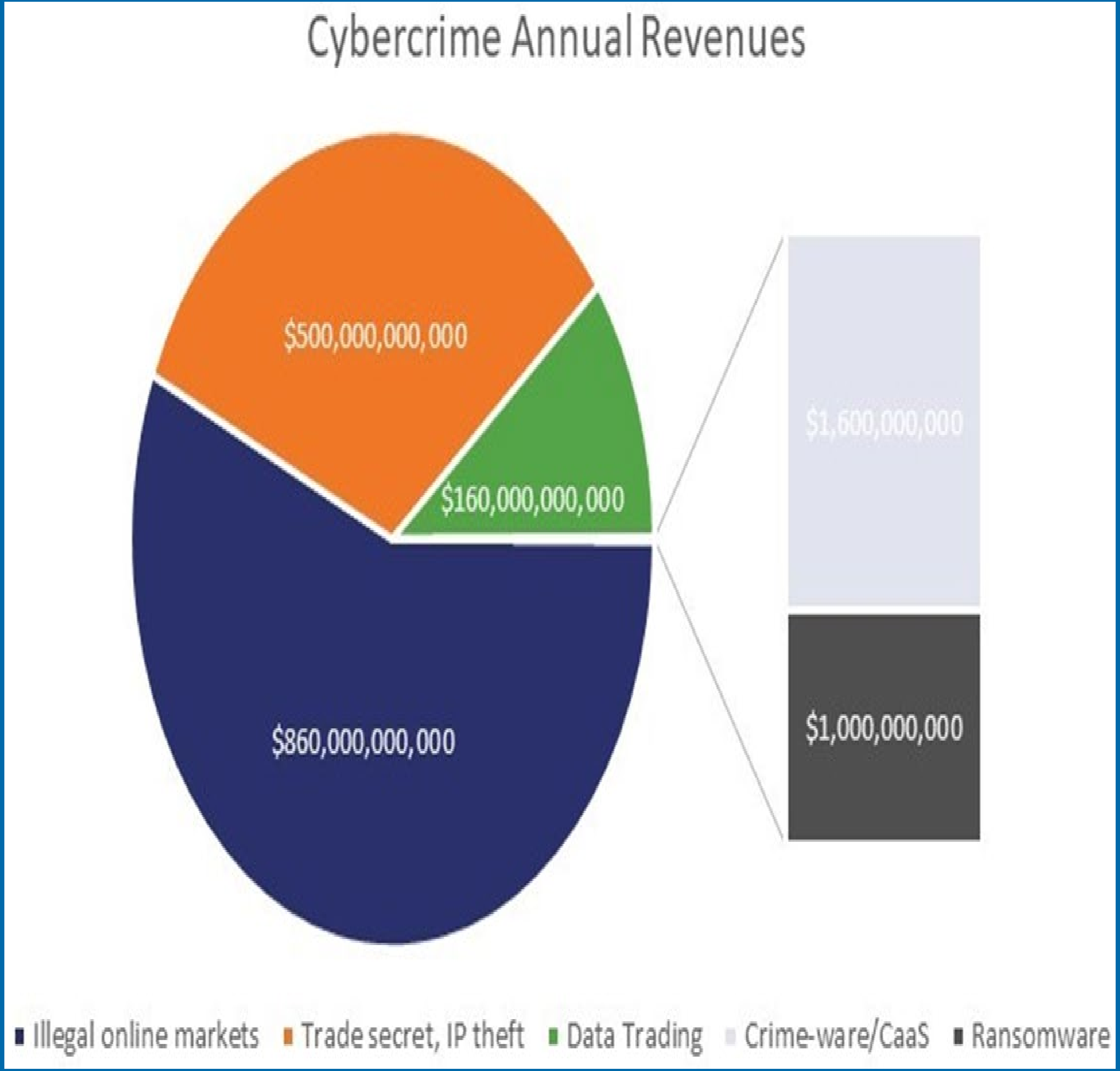


Why this is happening now

- Increasing technology use in all facets of our lives
- Scalable computing resources on-demand (cloud)
- Untraceable worldwide communications (encryption)
- Virtual international currency (cryptocurrency)
- And…

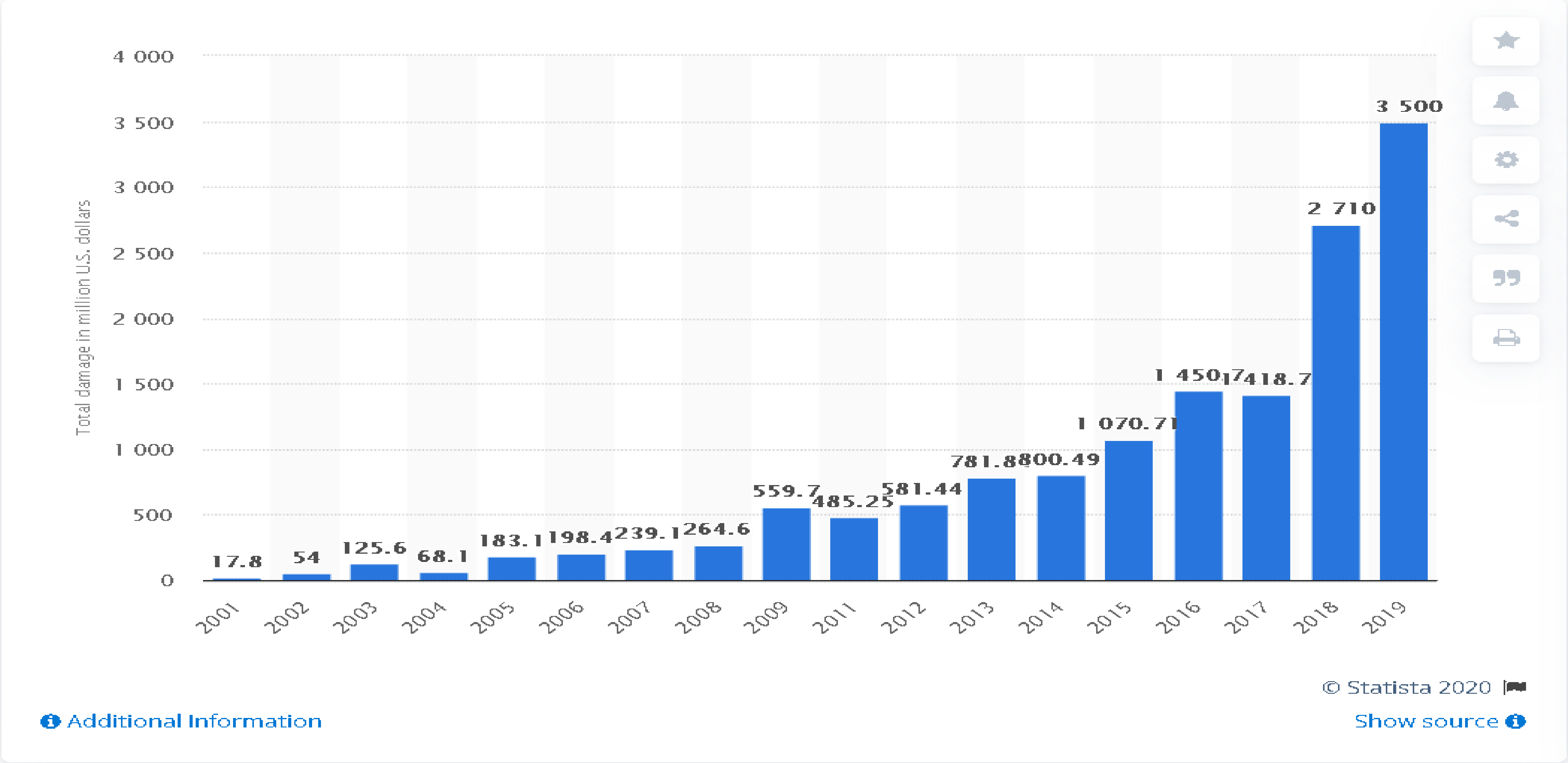
And… Crime has gone digital

- 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… Criminals are raking in money!

Cybercrime damage in $ per IC3



© Statista 2020

Additional Information

Show source

And… Threat actors vary

Changing Attacker Profiles

Recreational

- Fame and notoriety
- Limited technical resources
- Known exploits

Criminal

- Vandalism
- Limited technical capabilities

Hacktivist

- Statement
- Relentless, emotionally committed
- Vast networks
- Targeted attacks

Organized Crime

- Economic gain
- Significant technical resources and capabilities
- Established syndicates
- Adware, crimeware, IP theft

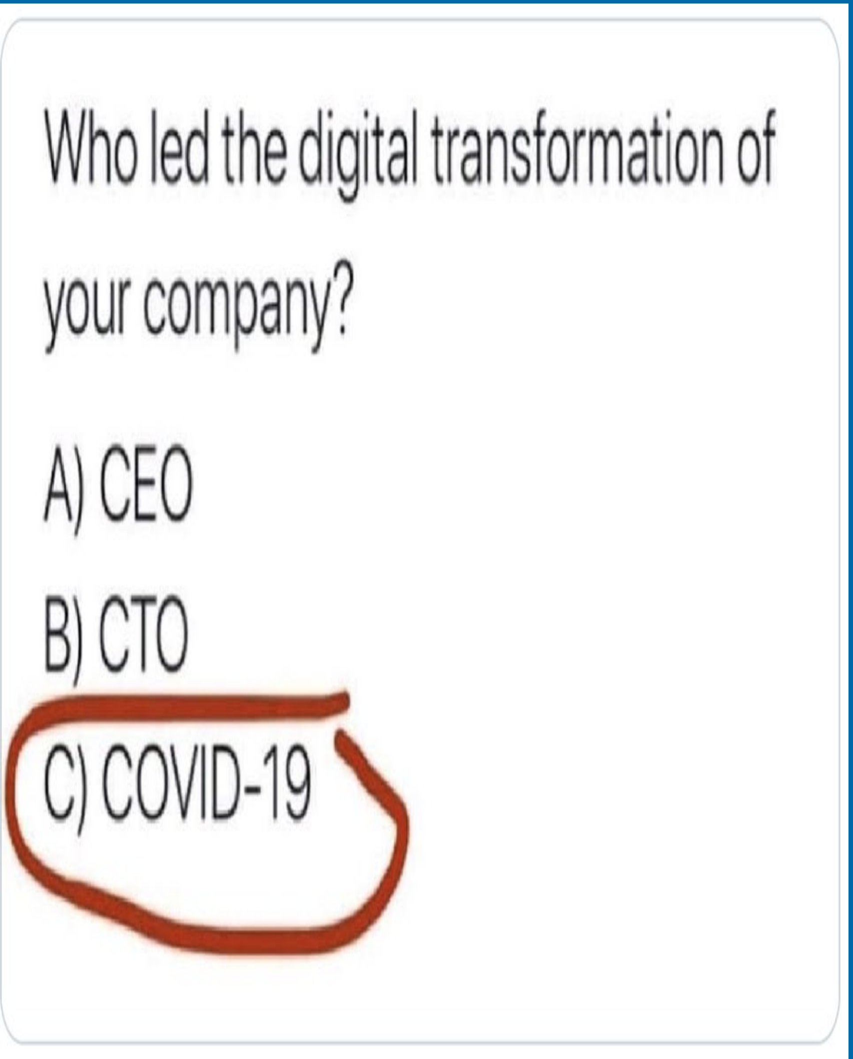
State Sponsored

- Cyberwar, state secrets, industrial espionage
- Highly sophisticated
- Nearly unlimited resources
- Advanced persistent threats

INCREASING RESOURCES AND SOPHISTICATION

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

And.. Digital transformation is upon us

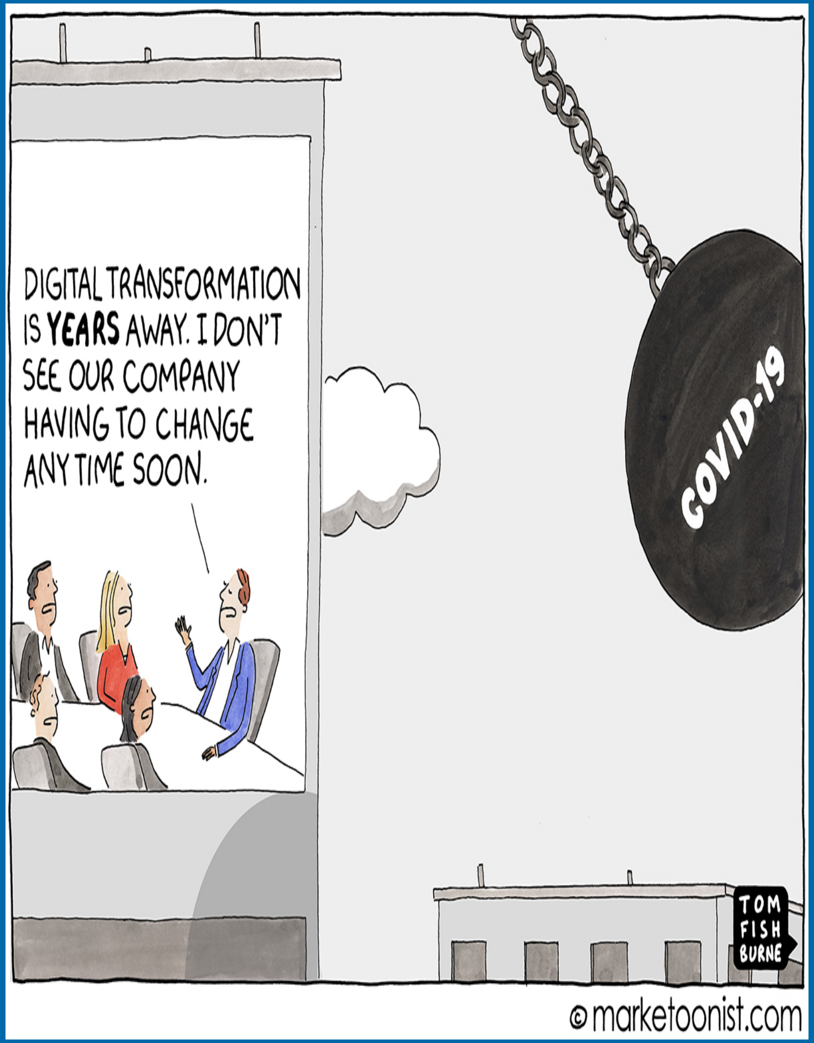


Who led the digital transformation of your company?

A) CEO

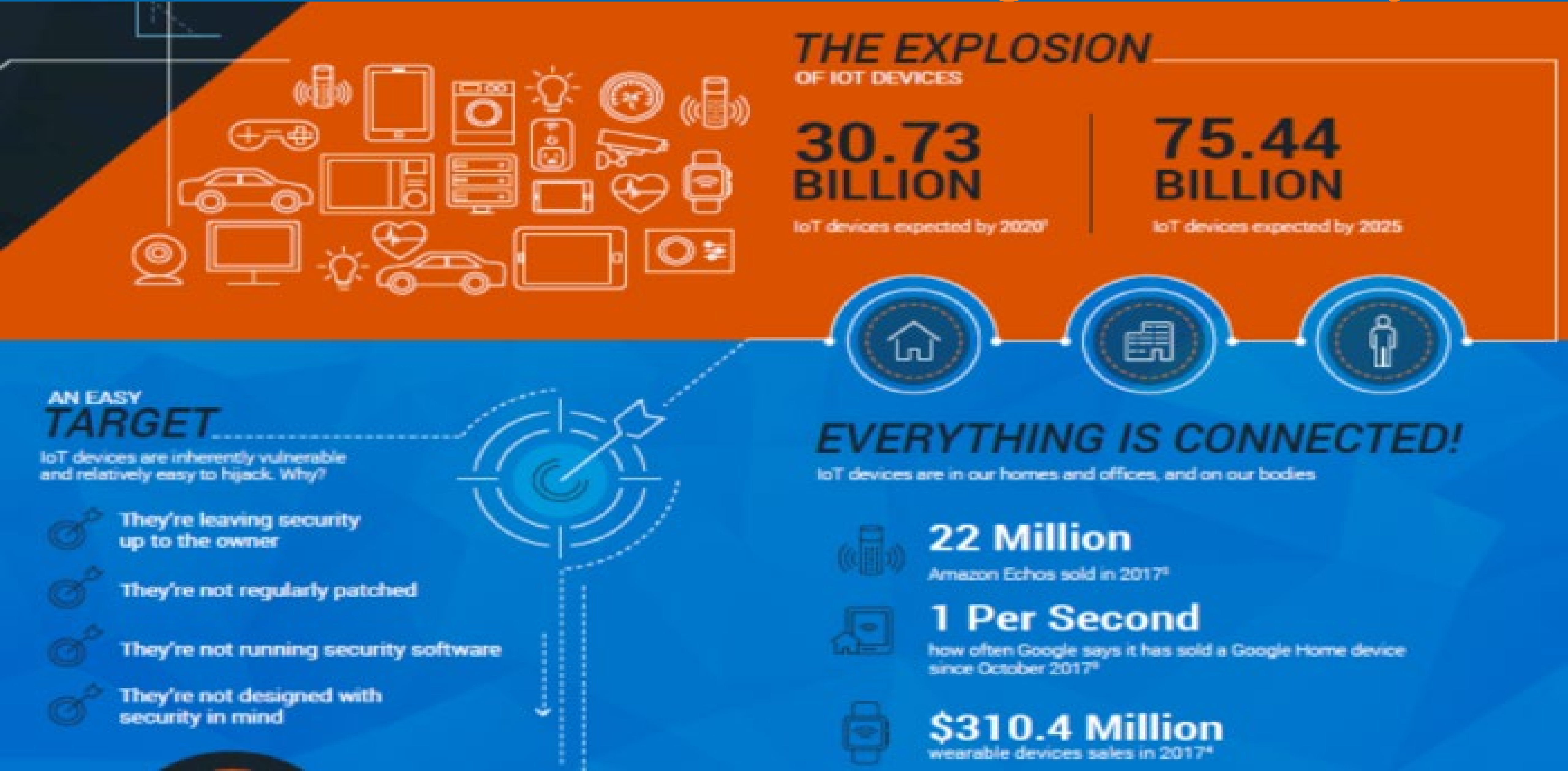
B) CTO

[✓ C) COVID-19]



DIGITAL TRANSFORMATION IS YEARS AWAY. I DON'T SEE OUR COMPANY HAVING TO CHANGE ANY TIME SOON.
COVID-19
TOM FISH BURNE
© marketoonist.com

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

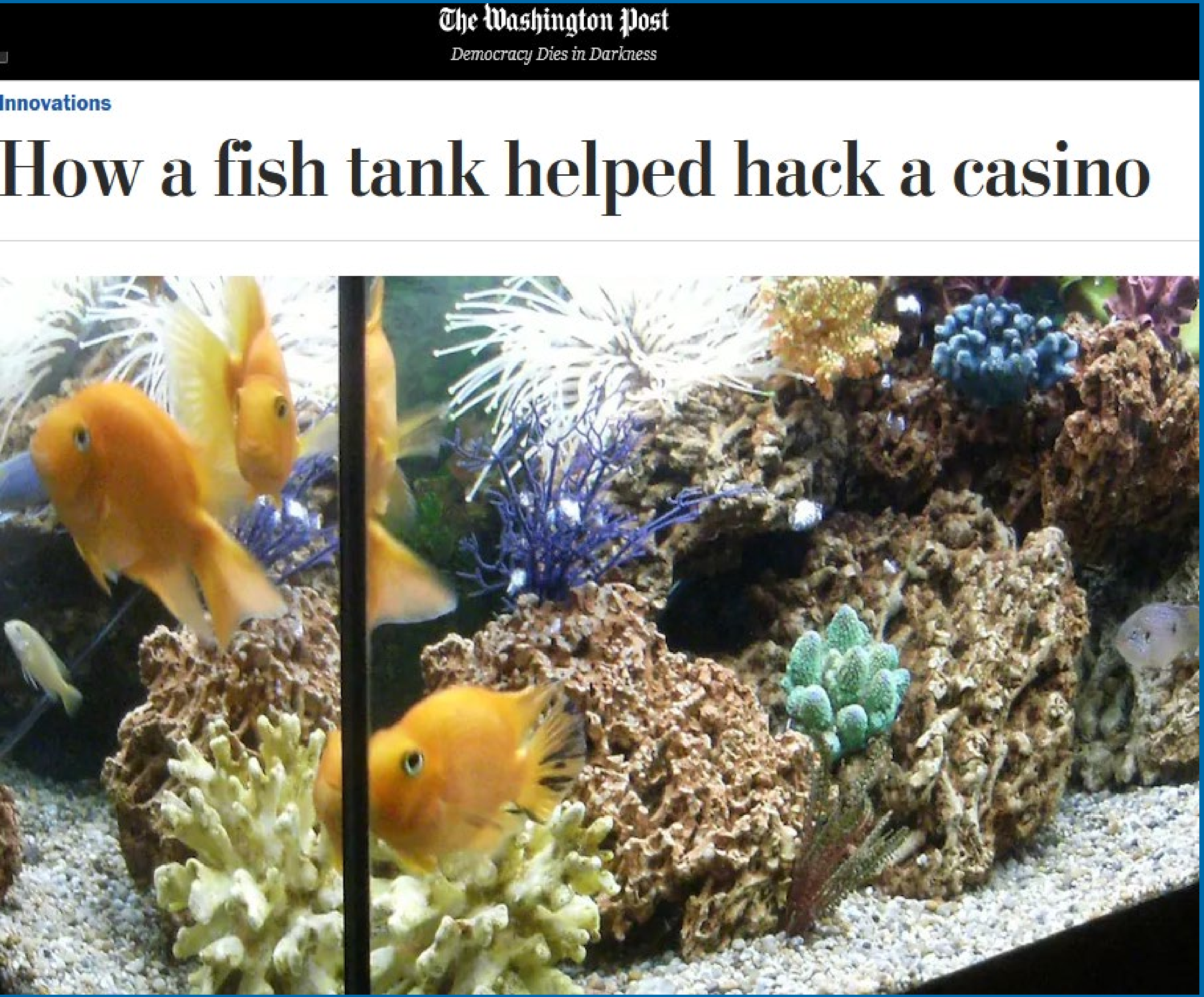
1 Per Second

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

$310.4 Million

wearable devices sales in 2017

And… The attack surface grows daily



The Washington Post

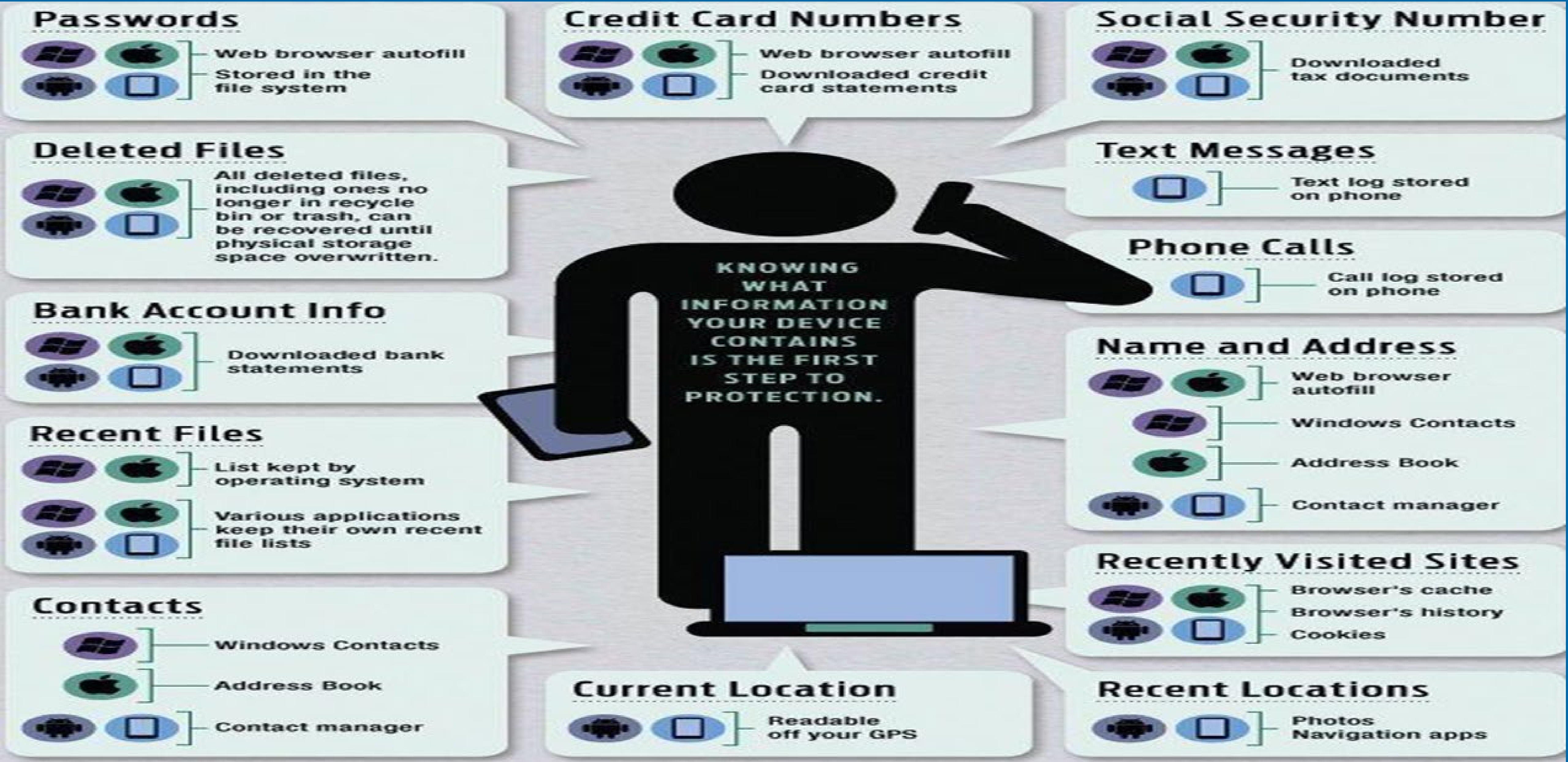
Democracy Dies in Darkness

Innovations

How a fish tank helped hack a casino

"CAN I INTEREST YOU IN A FIREWALL FOR YOUR TOASTER?"

And… Surveillance capitalism



KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.

Passwords
- Web browser autofill
- Stored in the file system

Credit Card Numbers
- Web browser autofill
- Downloaded credit card statements

Social Security Number
- Downloaded tax documents

Deleted Files
- All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Text Messages
- Text log stored on phone

Phone Calls
- Call log stored on phone

Bank Account Info
- Downloaded bank statements

Name and Address
- Web browser autofill
- Windows Contacts
- Address Book
- Contact manager

Recent Files
- List kept by operating system
- Various applications keep their own recent file lists

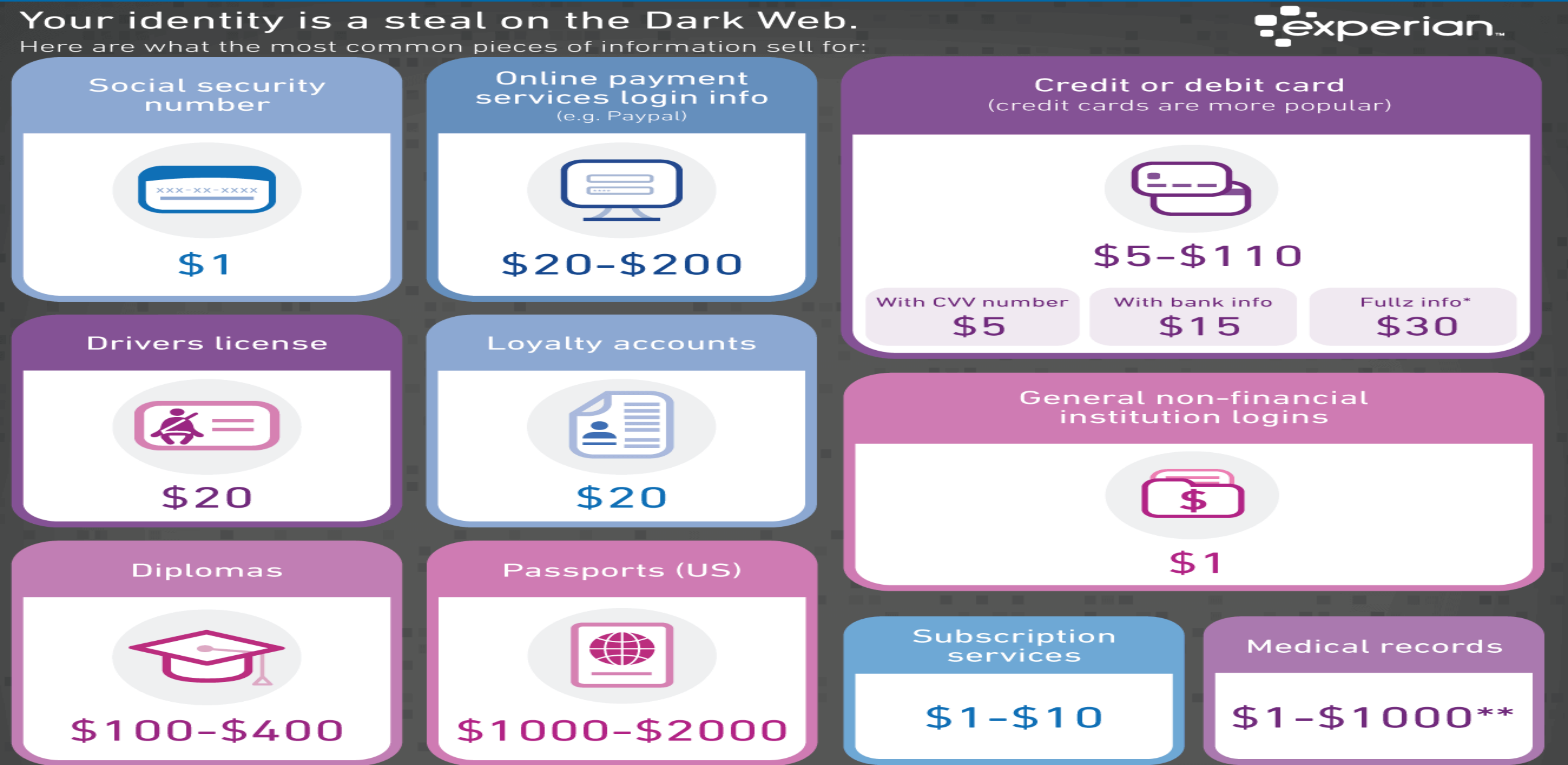
Recently Visited Sites
- Browser's cache
- Browser's history
- Cookies

Contacts
- Windows Contacts
- Address Book
- Contact manager

Current Location
- Readable off your GPS

Recent Locations
- Photos
- Navigation apps

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:

experian

Item	Price
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… 2020 Internet Minute

NETFLIX
404,444 hours of video streamed by users

TikTok
2,704 app installations

amazon
6,659 packages shipped

zoom
208,333 participants in meetings

319 new users gained

500 hours of video uploaded by users

347,222 stories

52,083 users connected

41.7m messages shared

28 new tracks added to library

Source: Visual Capitalist

statista

And… People are the weakest link

WHEN THE PRINCE OF NIGERIA CONTACTS YOU DIRECTLY
YOU DON'T ASK QUESTIONS; YOU HELP WHERE YOU CAN.
VIA 9GAG.COM
memegenerator.net

Scary things we've heard…

- "What do I care if someone gets the password to my email account? Hell let them have it. We lock our building at 6PM anyway so I'd like to see them try"- Client
- "Why would hackers go after me, I'm just a small business. Those were the words I used to say until last week when I got hit with Ransomware." – small business owner
- "Additionally, the gov collect software is password protected so the counter profile does not need to be password restricted." – Client

" WE'VE NARROWED OUR SECURITY RISKS DOWN to THESE TWO GROUPS."

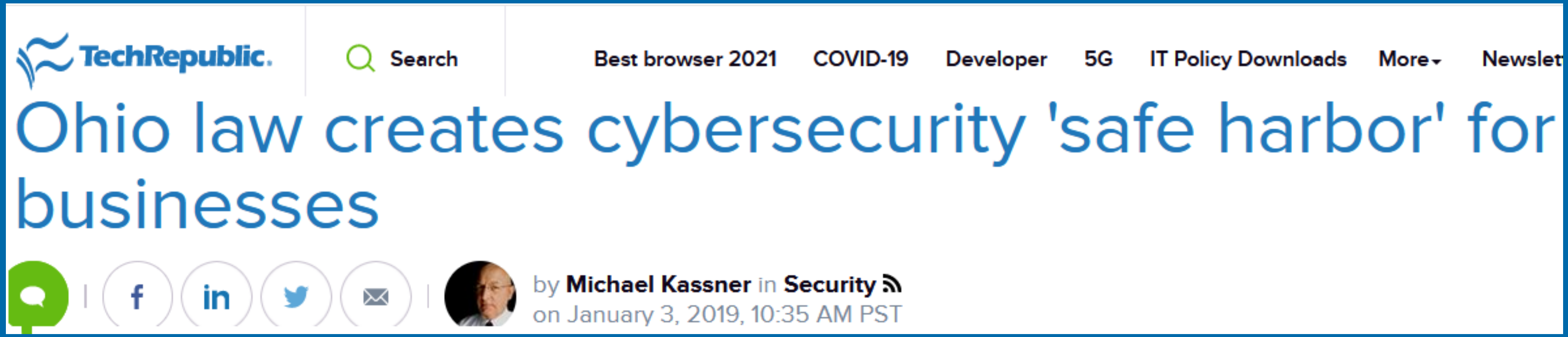
MY COMPUTER DOESN'T WORK! THE HARD DRIVE CRASHED! WHAT DO I DO?!
DID YOU BACK UP?
WHY? IS IT GONNA BLOW?!
WWW.WOOPHOTOS.COM

Guiding principals of security

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

Privacy & compliance needs growing

- Existing laws such as HIPPA require privacy
- New requirements from DoD require privacy and security
- New privacy laws such as GDPR and CCPA are creating new compliance concerns with huge potential fines
- Safe Harbor laws incentivize cybersecurity
- Lack of Due Diligence and/or Due Care can have devastating consequences



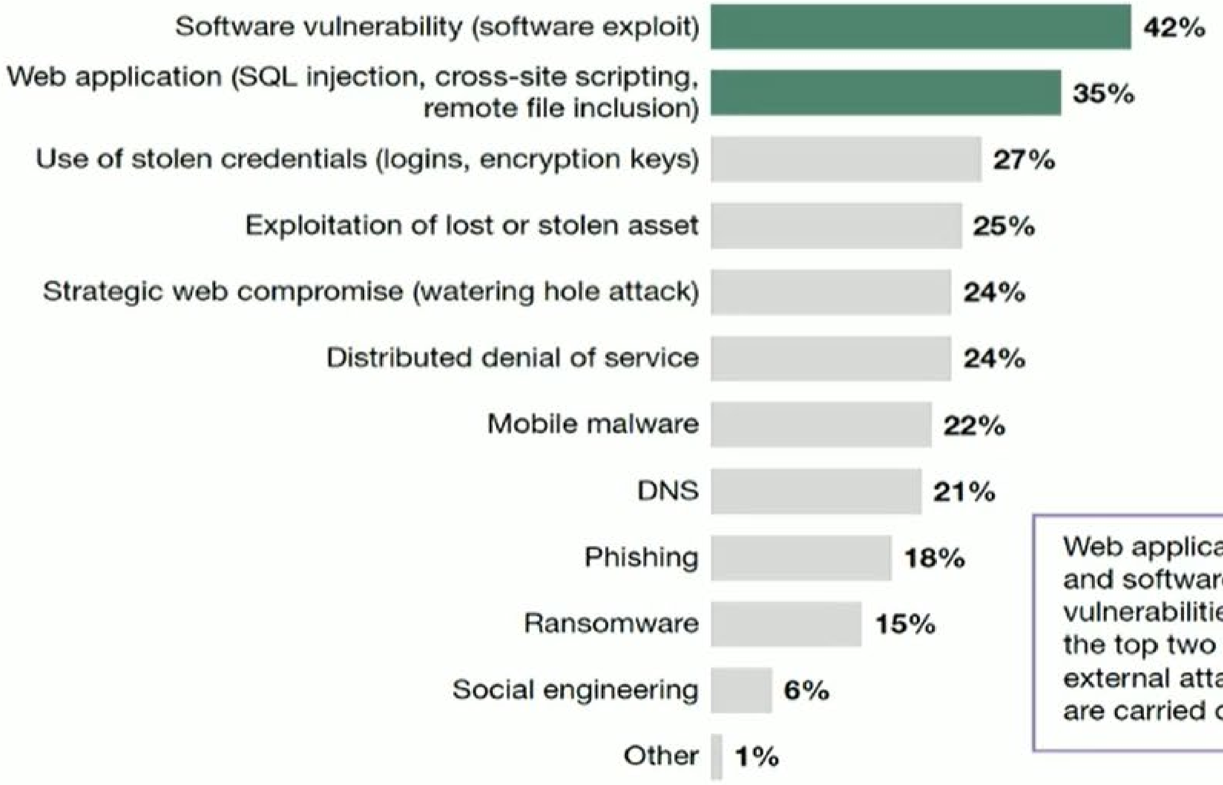
Ohio law creates cybersecurity 'safe harbor' for businesses

by Michael Kassner in Security
on January 3, 2019, 10:35 AM PST

Trends

The Prevalence of Breaches and Their Methodology

"How was the external attack carried out?"

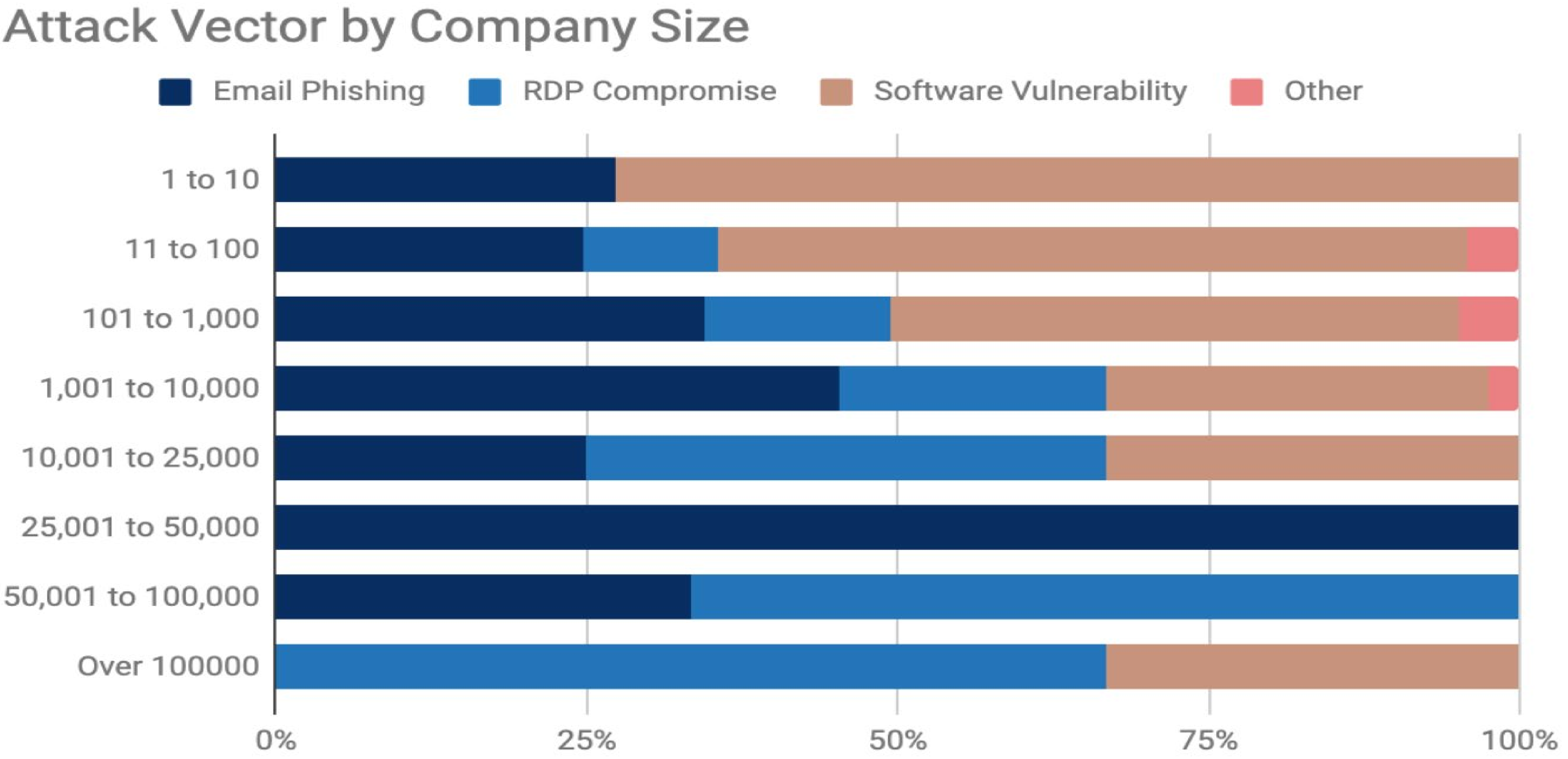


Web applications and software vulnerabilities are the top two ways external attacks are carried out.

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

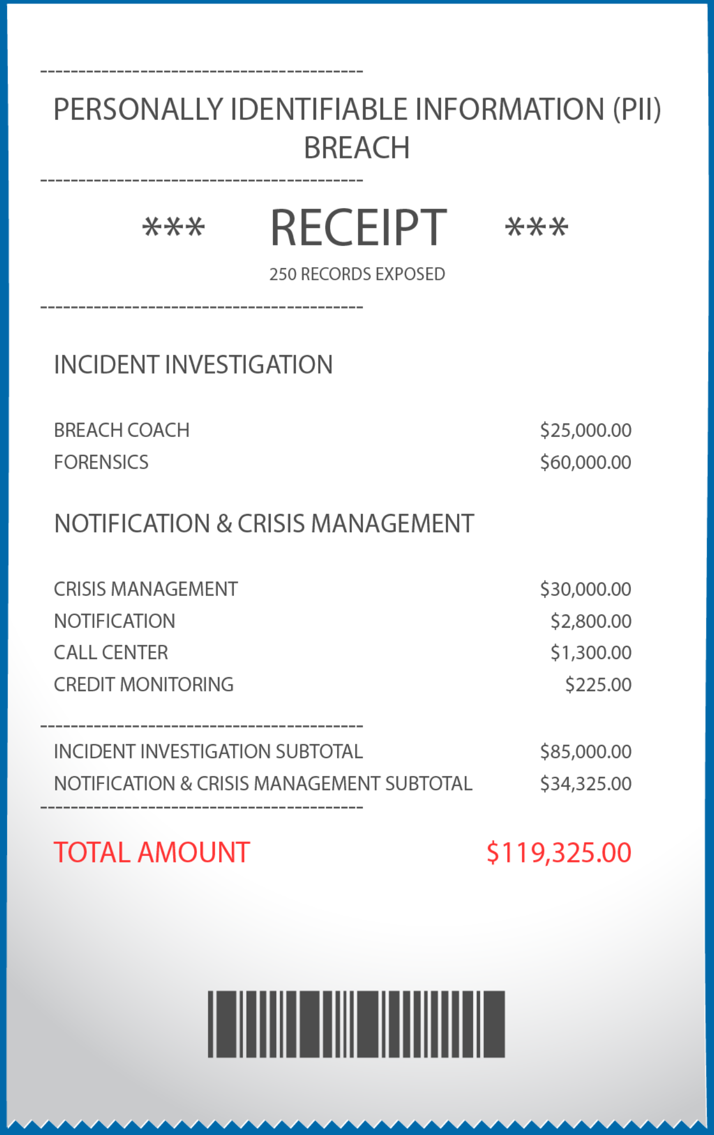
Trends



Attack Vector by Company Size
Email Phishing
RDP Compromise
Software Vulnerability
Other
1 to 10
11 to 100
101 to 1,000
1,001 to 10,000
10,001 to 25,000
25,001 to 50,000
50,001 to 100,000
Over 100000
0%
25%
50%
75%
100%

Incident costs are increasing!

- 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

Incident costs are increasing!

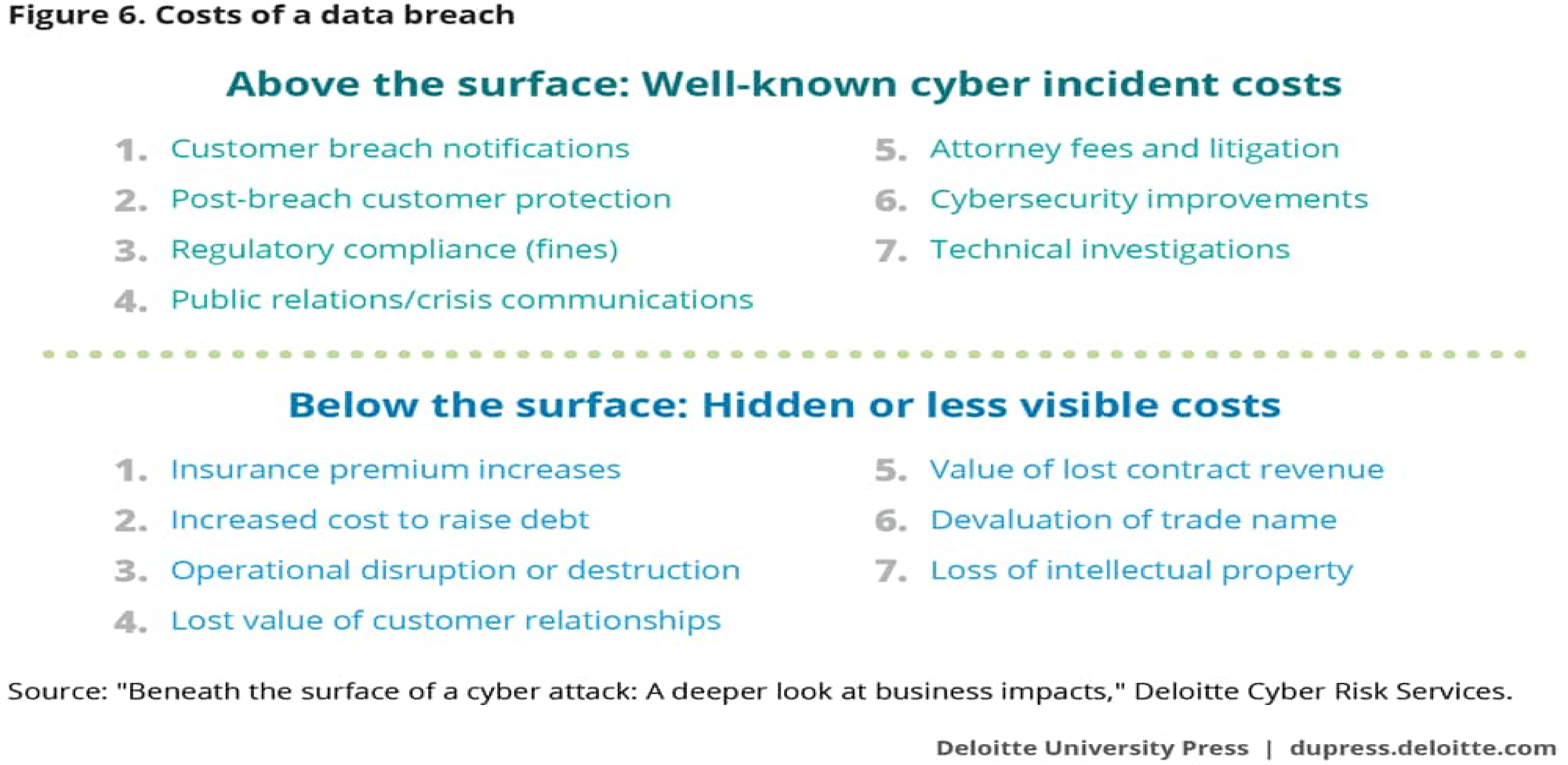


Figure 6. Costs of a data breach

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

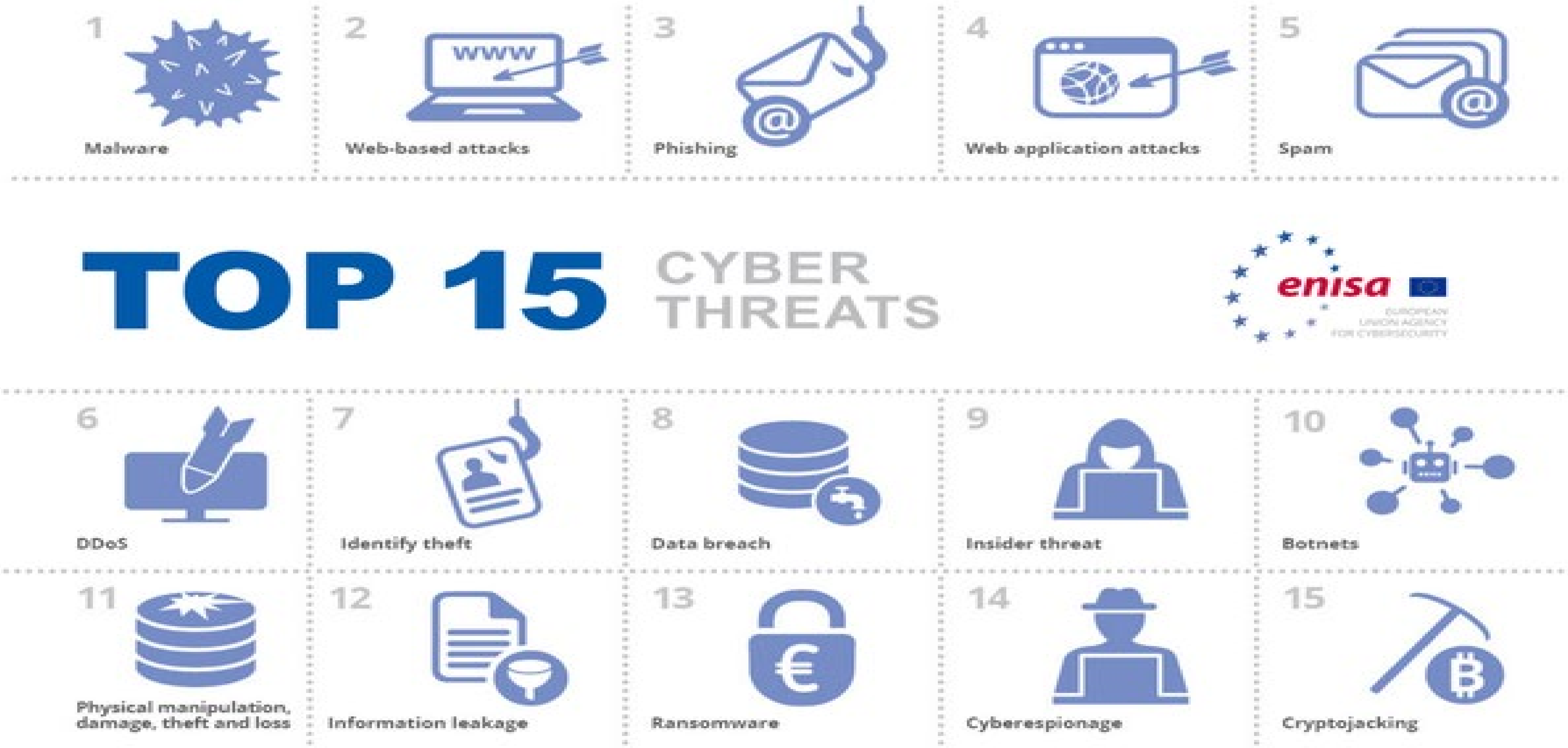
Below the surface: Hidden or less visible costs

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.

Deloitte University Press | dupress.deloitte.com

Threats



TOP 15 CYBER THREATS

1 Malware

2 Web-based attacks

3 Phishing

4 Web application attacks

5 Spam

6 DDoS

7 Identify theft

8 Data breach

9 Insider threat

10 Botnets

11 Physical manipulation, damage, theft and loss

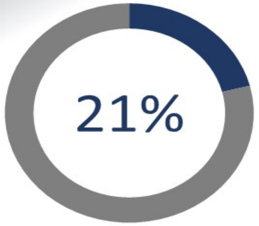
12 Information leakage

13 Ransomware

14 Cyberespionage

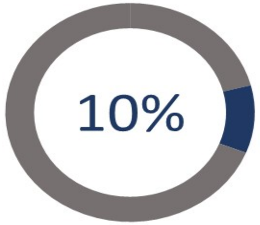
15 Cryptojacking

Root causes of cyber security incidents



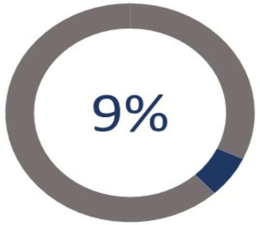
Abandoned Technology

Technology which is still in use but no longer actively managed and patched.



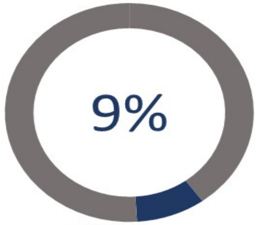
Versioning

Applying the wrong version of operating systems, applications, configurations, files, etc.



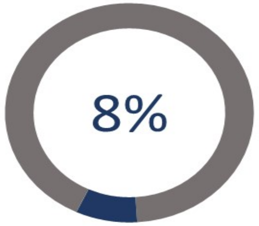
Access Management

Leaked or stolen credentials, escalated credentials, and failure to segregate role related rights.



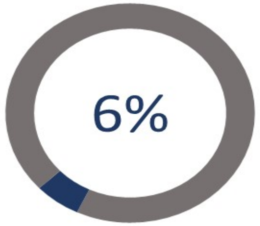
Technology Flaws

Security flaws and vulnerabilities in technology for which there are no patches available (yet).



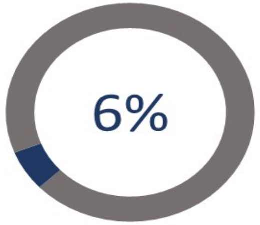
Copy/Paste Flaws

Flaws and vulnerabilities caused by copying wrong files, configurations, etc.



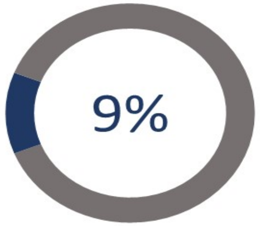
Skills

Lack of skills to properly configure and manage the technology.



Unencrypted

Unencrypted confidential or privacy related information left accessible/vulnerable.



Usage

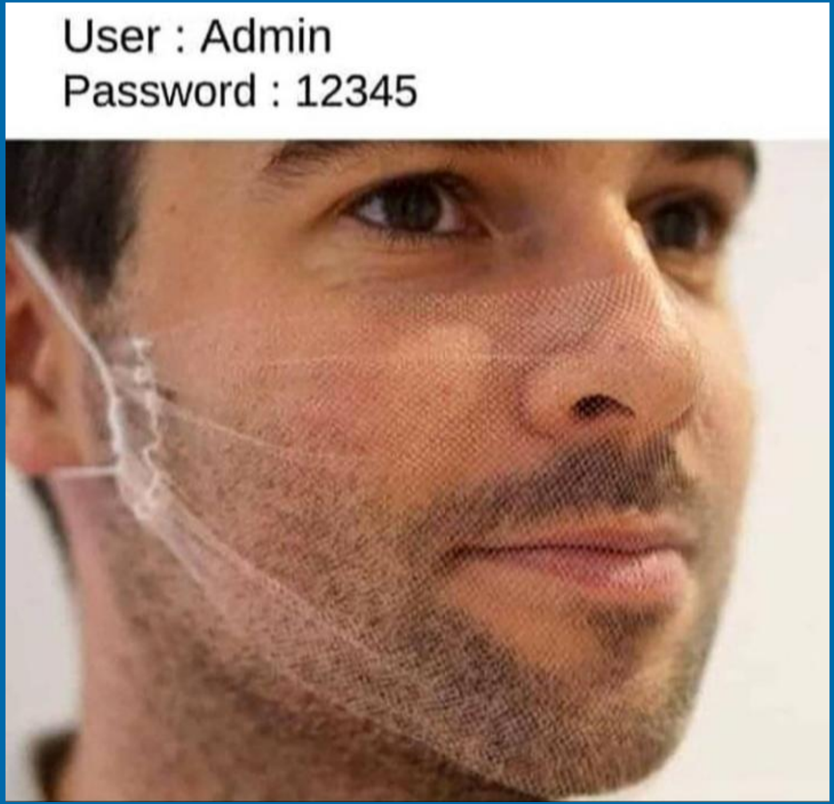
Flaws and vulnerabilities caused by copying wrong files, configurations, etc.

3 simple steps to remember

- Stop
- Think
- Protect – Be a human firewall

Threats: Poor credential management

I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."



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

Threats: Unpatched Software

- A Ponemon Institute survey found 57% of security breaches were due to vulnerabilities in unpatched software
- 34% of these cybercrime victims were aware of holes but didn’t patch them in time.
- 37% of breach victims don’t perform regular scans to find vulnerabilities in their own systems
    - Patching gaps are an issue:
        - Some IT teams are unaware of the updates that are available
        - Some know these updates are available, but don’t have the resources or strategies implement the patches

Threats: Spoofing

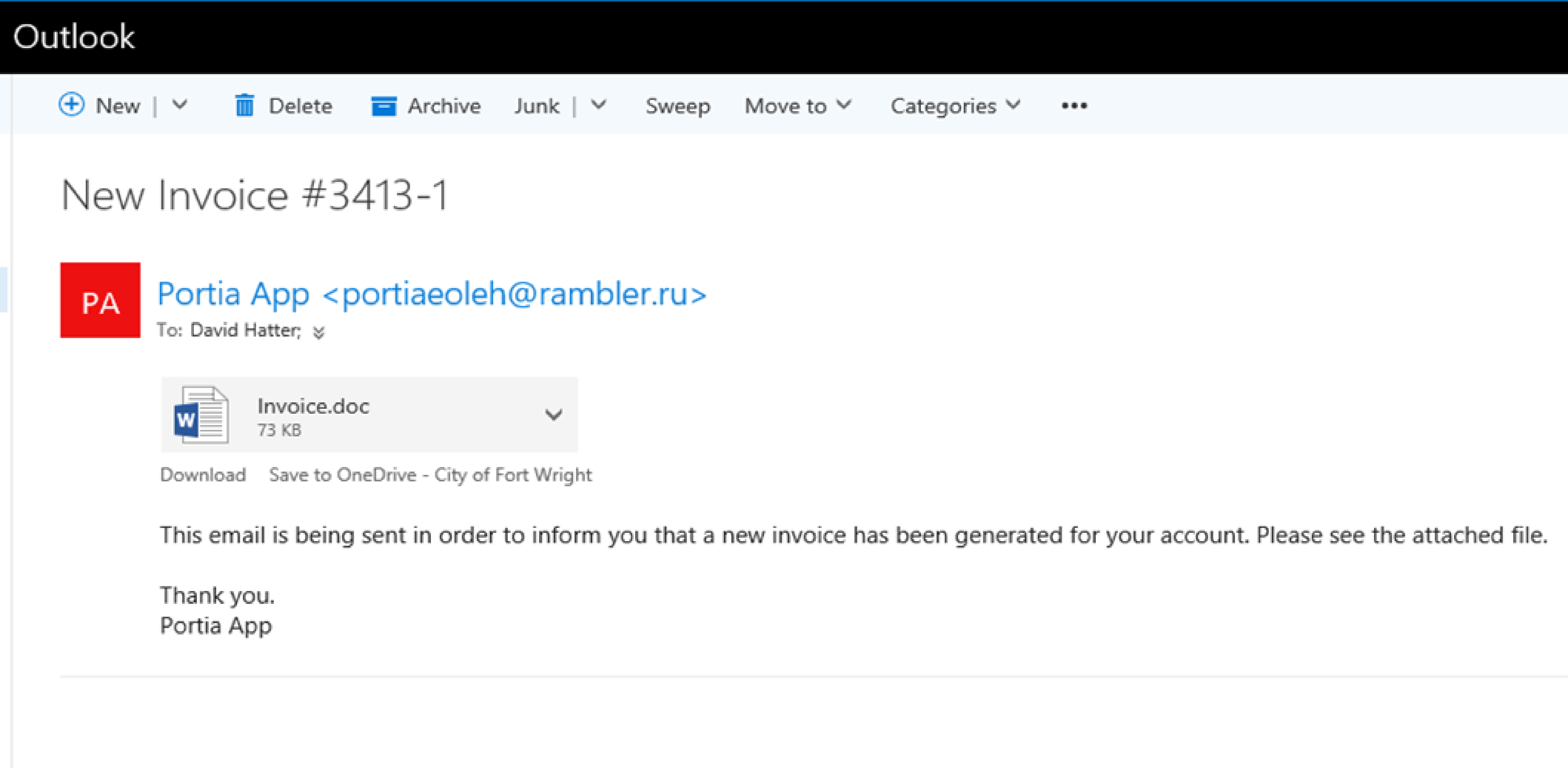
- "Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security." – Techopedia
- Spoofing leads to:
  - Phishing
  - Vishing (Voice based)
  - Smishing (Text based)
  - Doppleganger or Lookalike websites

Threats: 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

MY BANK JUST EMAILED ME
BETTER CONFIRM MY ADDRESS AND SOCIAL SECURITY NUMBER LIKE THEY ASKED
quickmeme.com

Threats: Phishing



New Invoice #3413-1

PA

Portia App <portiaeoleh@rambler.ru>

To: David Hatter;

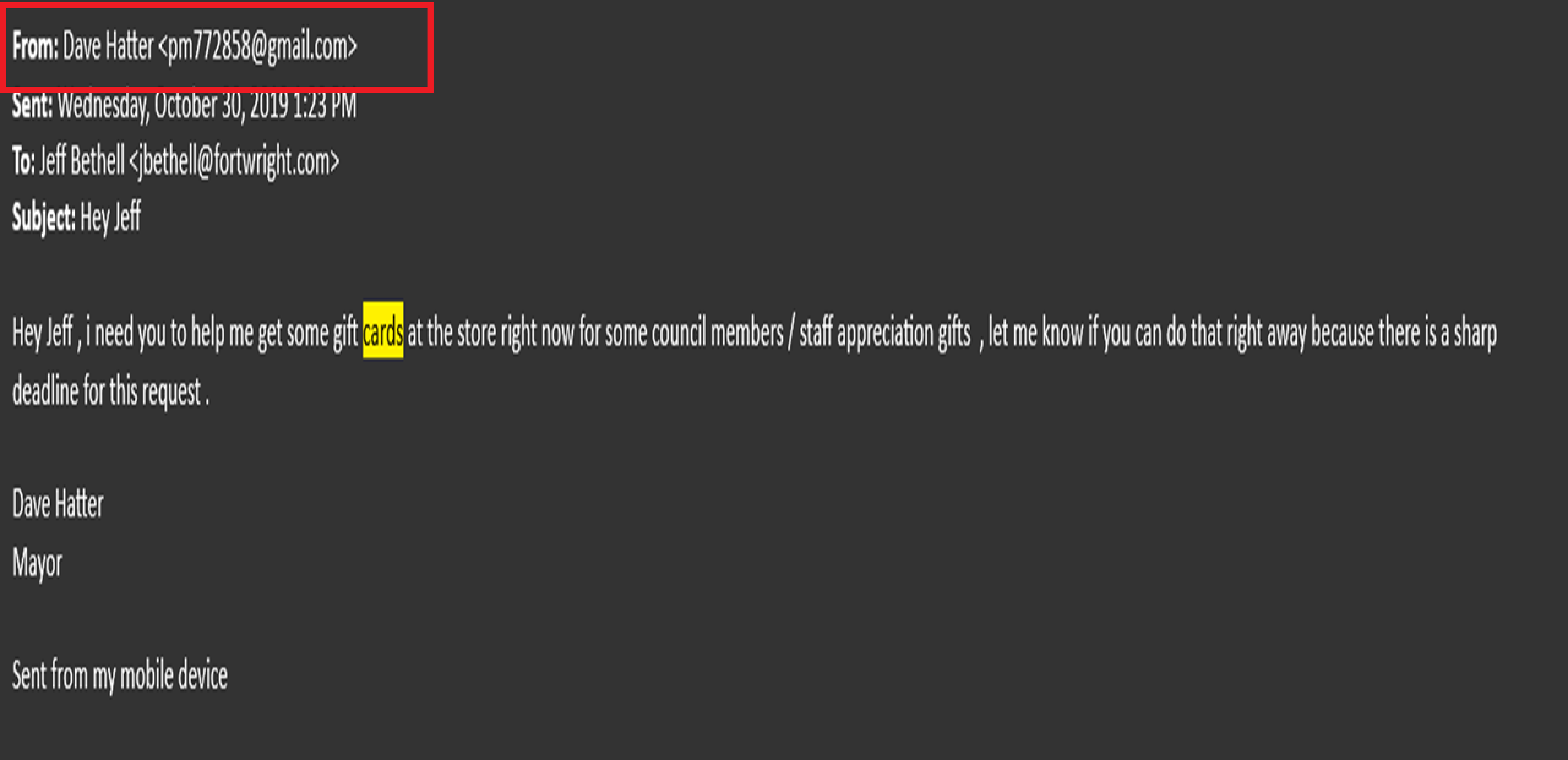
Invoice.doc
73 KB

Download Save to OneDrive - City of Fort Wright

This email is being sent in order to inform you that a new invoice has been generated for your account. Please see the attached file.

Thank you.
Portia App

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

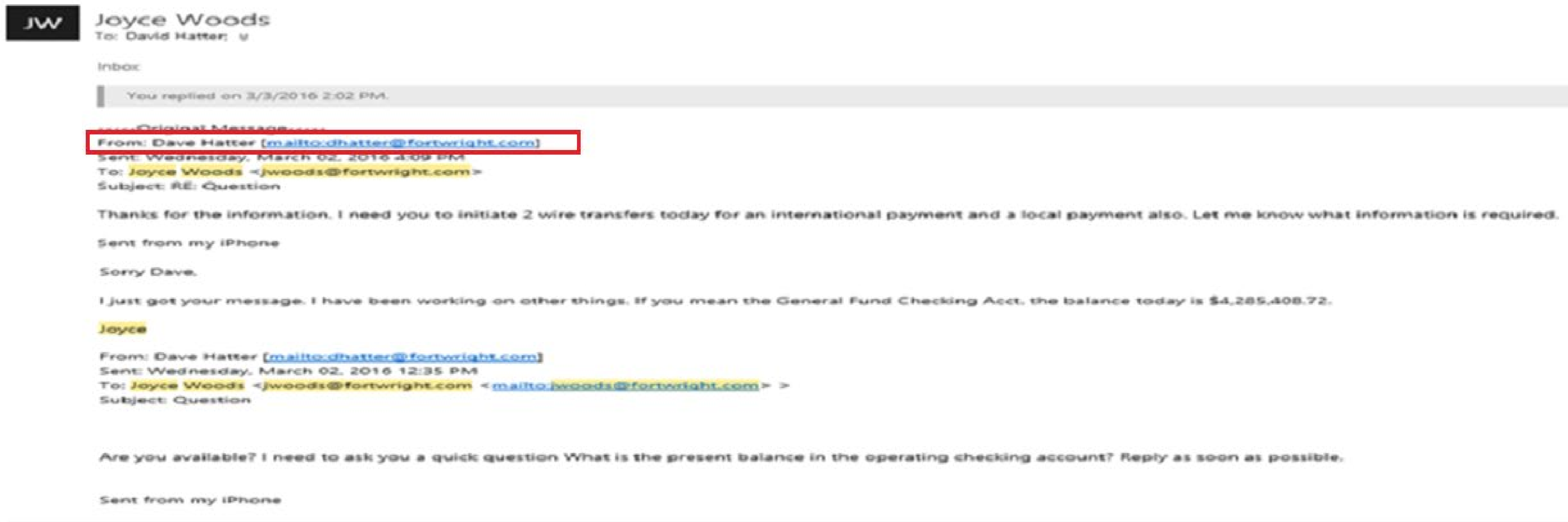
Hey Jeff , i need you to help me get some gift cards at the store right now for some council members / staff appreciation gifts , let me know if you can do that right away because there is a sharp deadline for this request .

Dave Hatter

Mayor

Sent from my mobile device

Threats: Phishing



JW

Joyce Woods

To: David Hatter;

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.

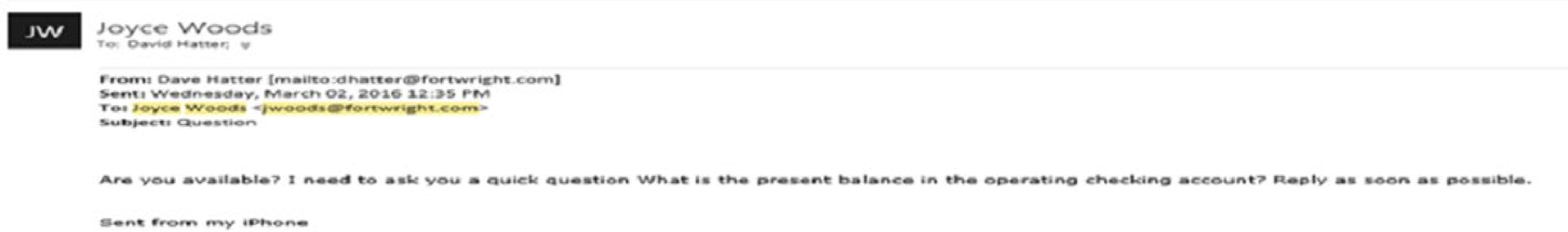
I just got your message. I have been working on other things. If you mean the General Fund Checking Acct. the balance today is $4,285,408.72.

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

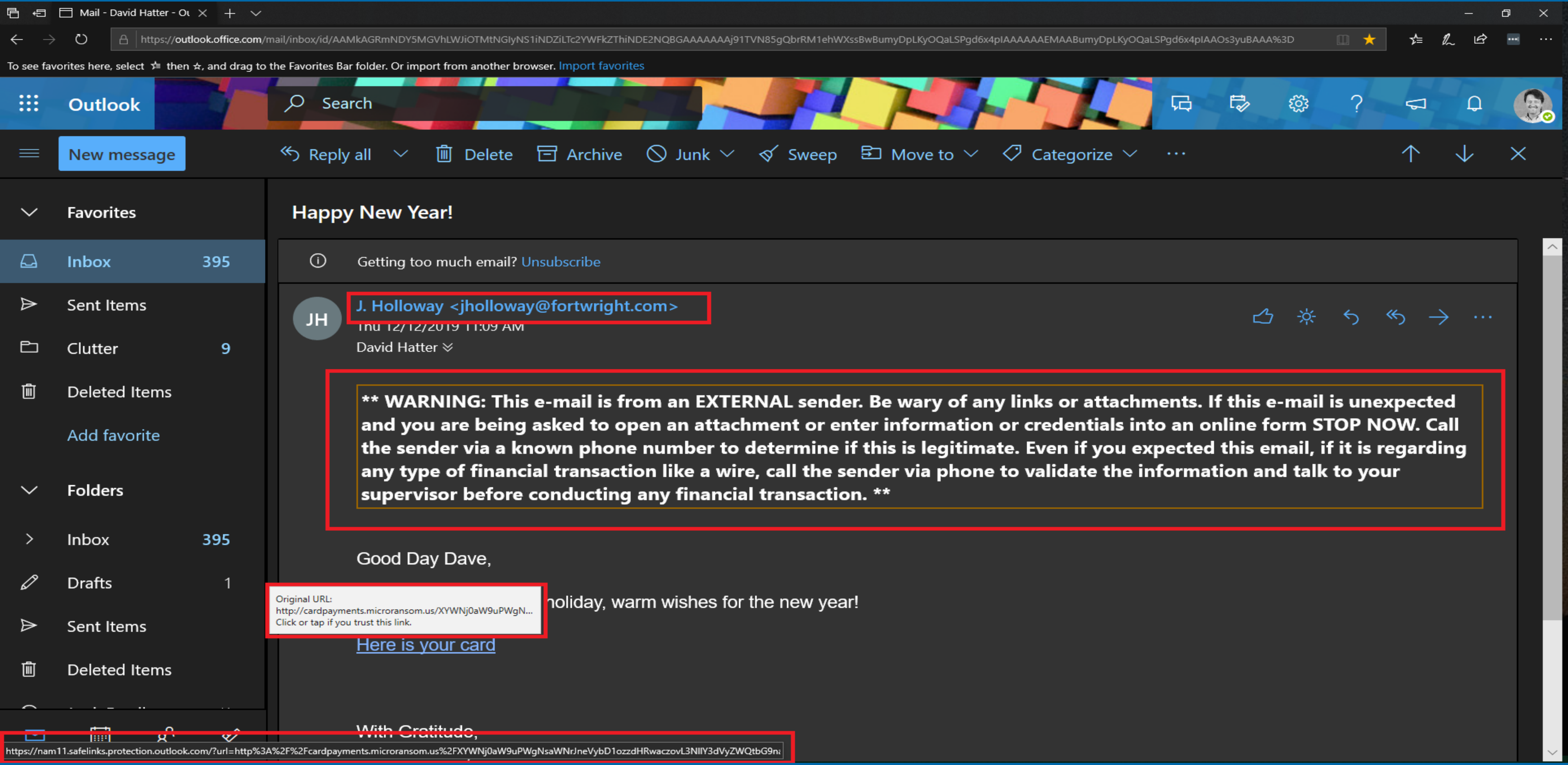
To: David Hatter;

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: Phishing



https://outlook.office.com/mail/inbox/id/AAMkAGRmNDY5MGVhLWJiOTMtNGIyNS1iNDZiLTc2YWFkZThiNDE2NQBGAAAAAAAj91TVN85gQbrRM1ehWXssBwBumyDpLKyOQaLSPgd6x4pIAAAAAAEMAABumyDpLKyOQaLSPgd6x4pIAAOs3yuBAAA%3D

To see favorites here, select ☆ then ☆, and drag to the Favorites Bar folder. Or import from another browser. Import favorites

Happy New Year!

Getting too much email? Unsubscribe

J. Holloway <jholloway@fortwright.com>

Thu 12/12/2019 11:09 AM

David Hatter

**** WARNING: This e-mail is from an EXTERNAL sender. Be wary of any links or attachments. If this e-mail is unexpected and you are being asked to open an attachment or enter information or credentials into an online form STOP NOW. Call the sender via a known phone number to determine if this is legitimate. Even if you expected this email, if it is regarding any type of financial transaction like a wire, call the sender via phone to validate the information and talk to your supervisor before conducting any financial transaction. ****

Good Day Dave,

holiday, warm wishes for the new year!

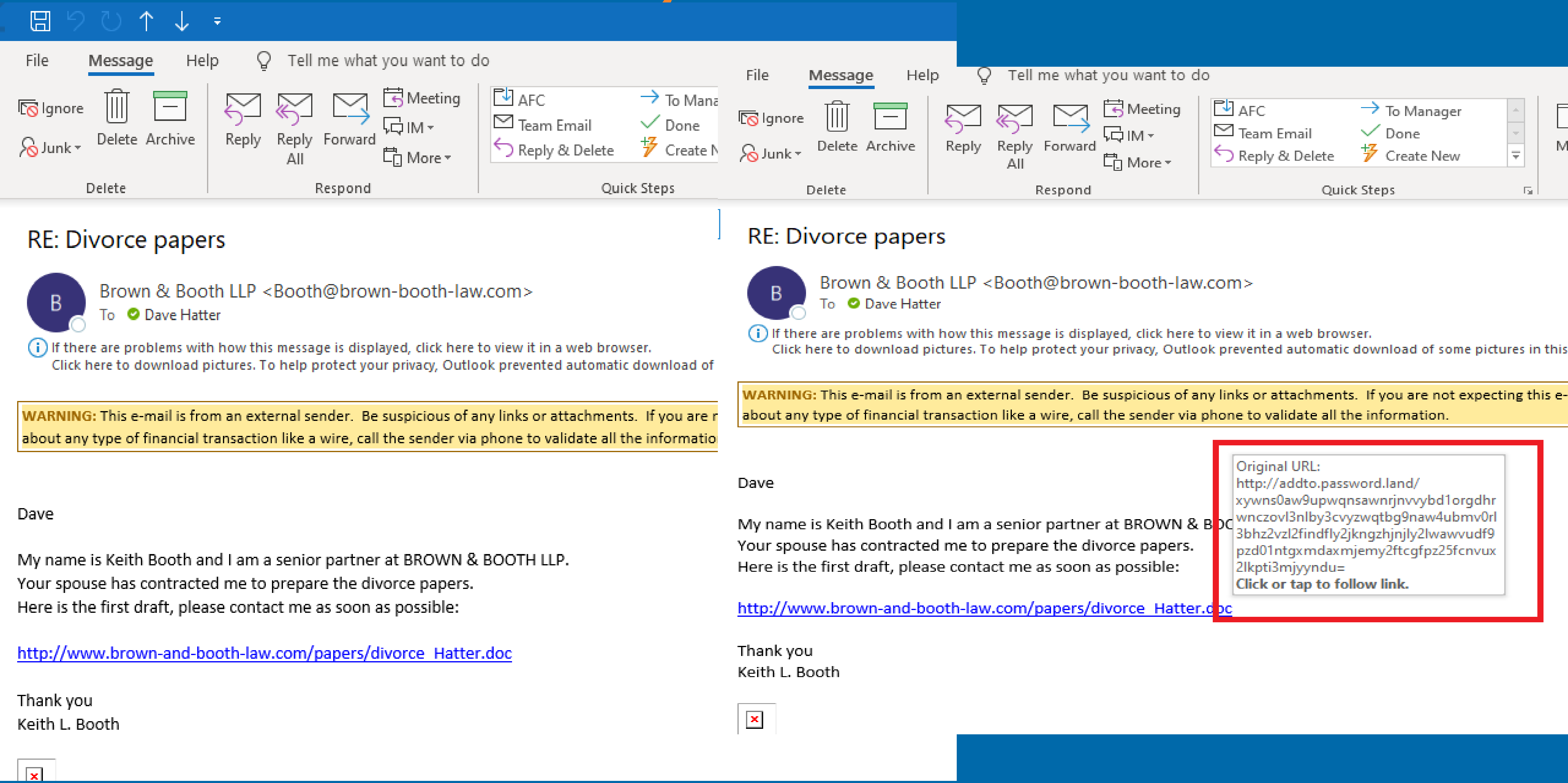
Original URL:
http://cardpayments.microransom.us/XYWNj0aW9uPWgN...
Click or tap if you trust this link.

Here is your card

With Gratitude,

https://nam11.safelinks.protection.outlook.com/?url=http%3A%2F%2Fcardpayments.microransom.us%2FXYWNj0aW9uPWgNsaWNrJneVybD1ozzdHRwaczovL3NlIY3dVyZWQtbG9n

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

WARNING: This e-mail is from an external sender. Be suspicious of any links or attachments. If you are n
about any type of financial transaction like a wire, call the sender via phone to validate all the informatio

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

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

Dave

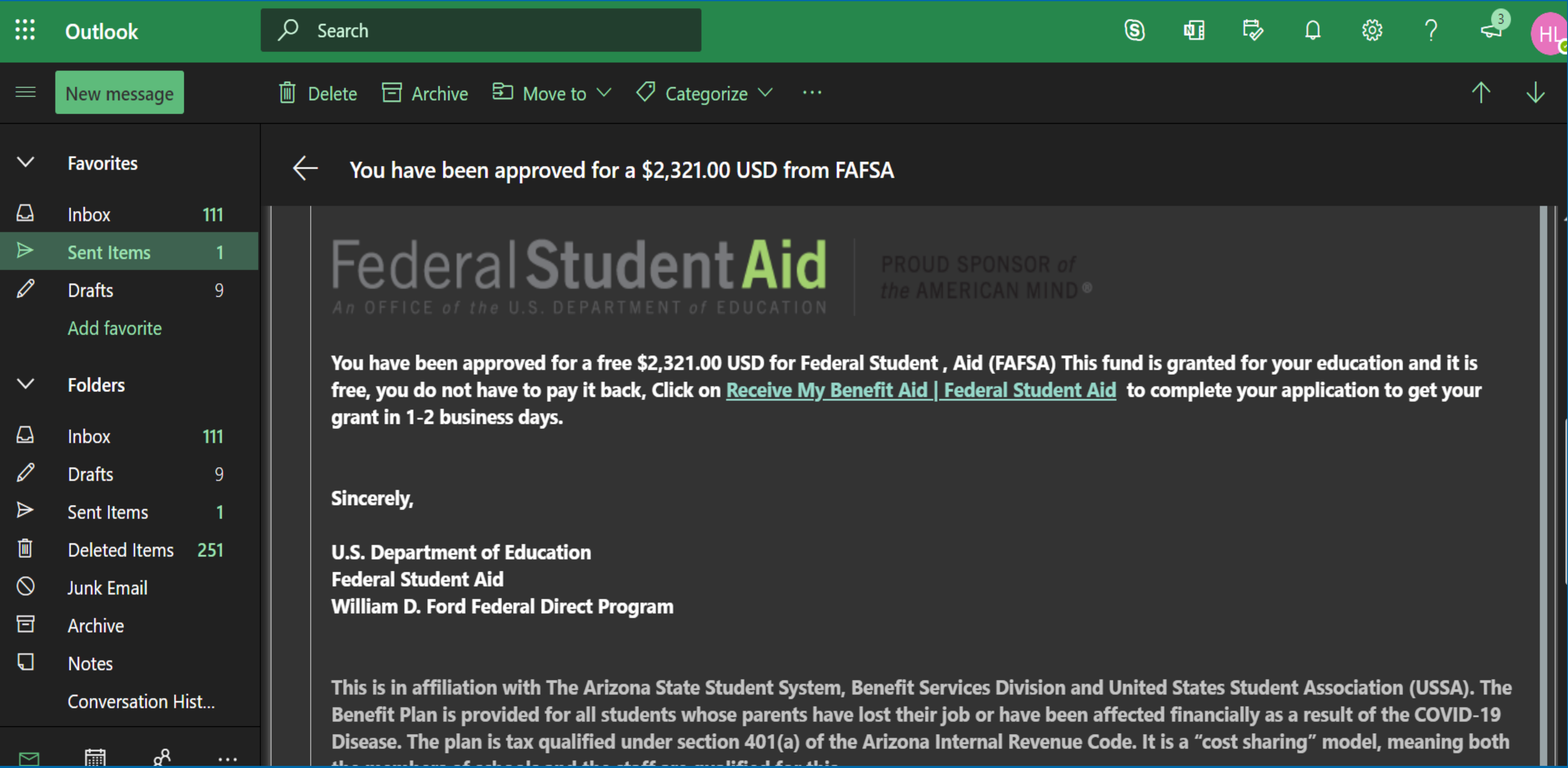
My name is Keith Booth and I am a senior partner at BROWN & BOO
Your spouse has contracted me to prepare the divorce papers.
Here is the first draft, please contact me as soon as possible:

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

Thank you
Keith L. Booth

Original URL:
http://addto.password.land/
xywns0aw9upwqnsawnrjnvvybd1orgdhr
wnczovl3nlby3cvyzwqtbg9naw4ubmv0rl
3bhz2vzl2findfly2jkngzhjnjly2lwawvudf9
pzd01ntgxmdaxmjemy2ftcgfpz25fcnvux
2lkpti3mjyyndu=
Click or tap to follow link.

Threats: Phishing



You have been approved for a $2,321.00 USD from FAFSA

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
PROUD SPONSOR of the AMERICAN MIND®

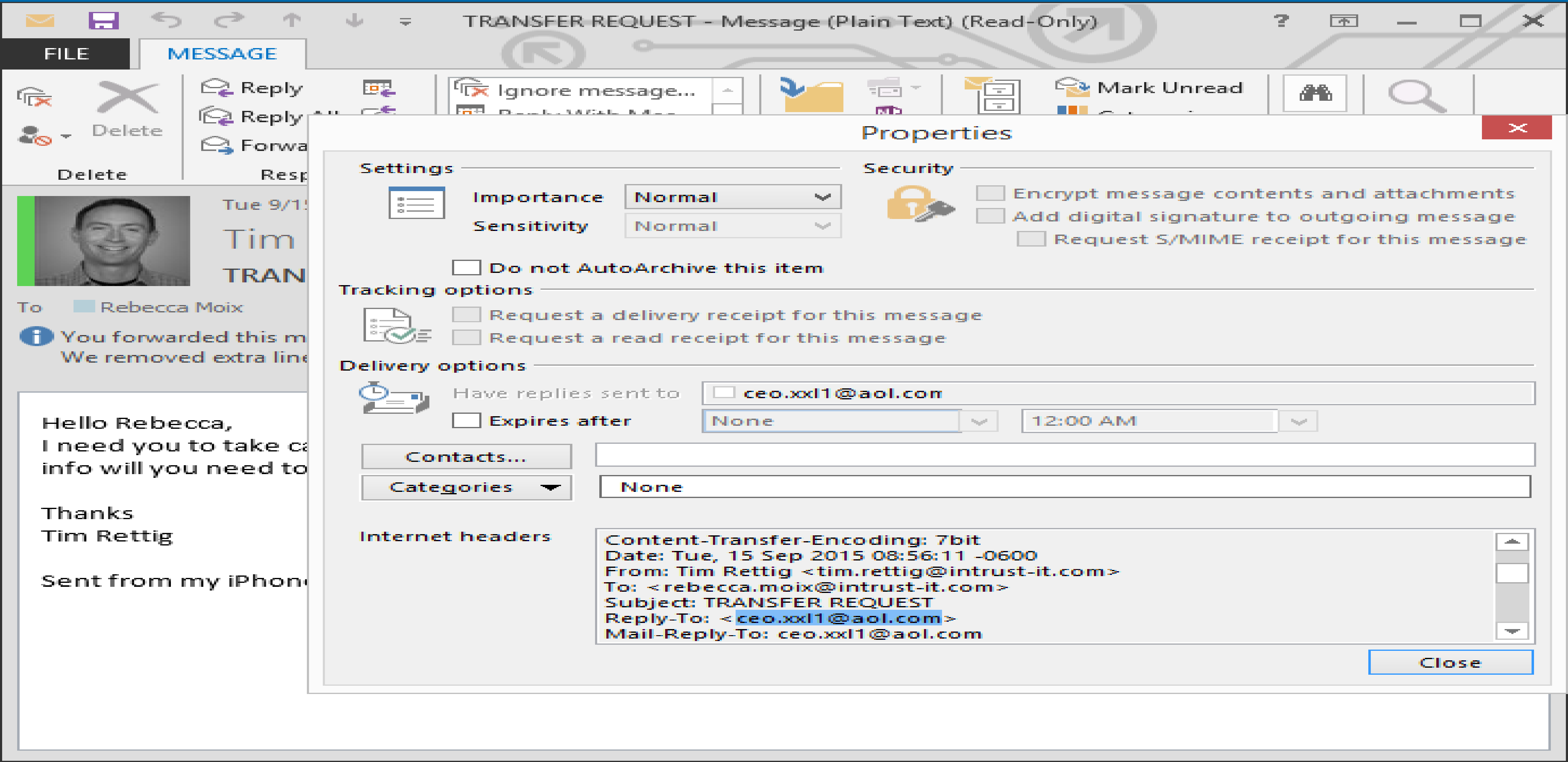
You have been approved for a free $2,321.00 USD for Federal Student , Aid (FAFSA) This fund is granted for your education and it is free, you do not have to pay it back, Click on Receive My Benefit Aid | Federal Student Aid to complete your application to get your grant in 1-2 business days.

Sincerely,

U.S. Department of Education
Federal Student Aid
William D. Ford Federal Direct Program

This is in affiliation with The Arizona State Student System, Benefit Services Division and United States Student Association (USSA). The Benefit Plan is provided for all students whose parents have lost their job or have been affected financially as a result of the COVID-19 Disease. The plan is tax qualified under section 401(a) of the Arizona Internal Revenue Code. It is a "cost sharing" model, meaning both the members of schools and the staff are qualified for this

Threats: Phishing



TRANSFER REQUEST - Message (Plain Text) (Read-Only)

Tue 9/15

Tim

TRAN

To Rebecca Moix

You forwarded this m
We removed extra line

Hello Rebecca,
I need you to take ca
info will you need to

Thanks
Tim Rettig

Sent from my iPhone

Importance: Normal
Sensitivity: Normal

□ Encrypt message contents and attachments
□ Add digital signature to outgoing message
□ Request S/MIME receipt for this message

□ Do not AutoArchive this item

□ Request a delivery receipt for this message
□ Request a read receipt for this message

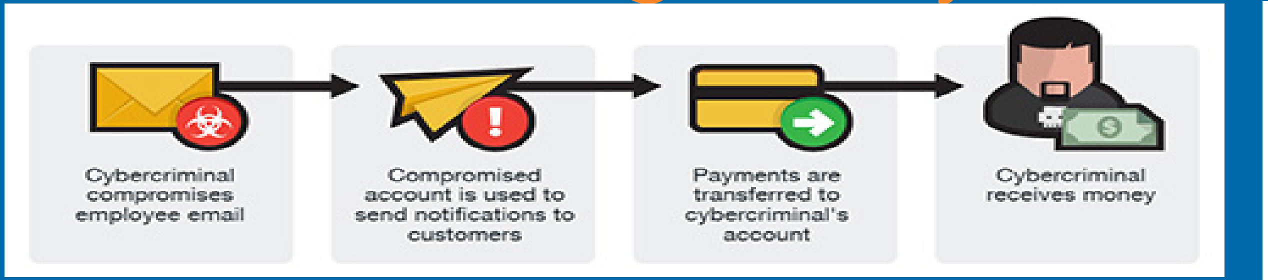
Have replies sent to: ceo.xxl1@aol.com
□ Expires after: None 12:00 AM

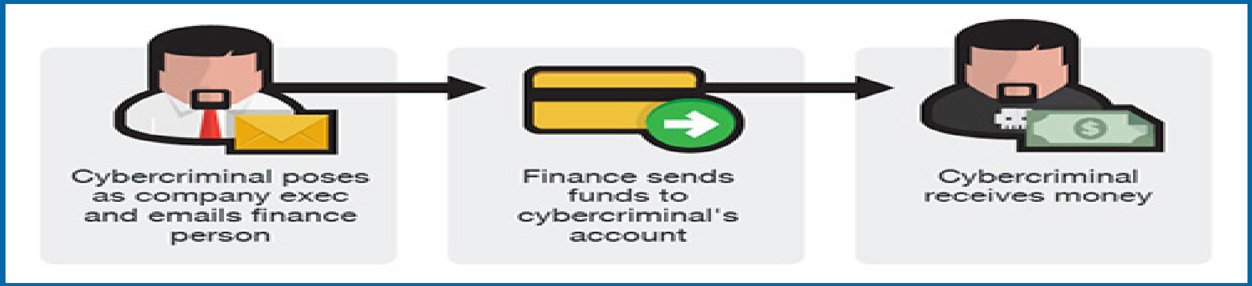
Categories: None

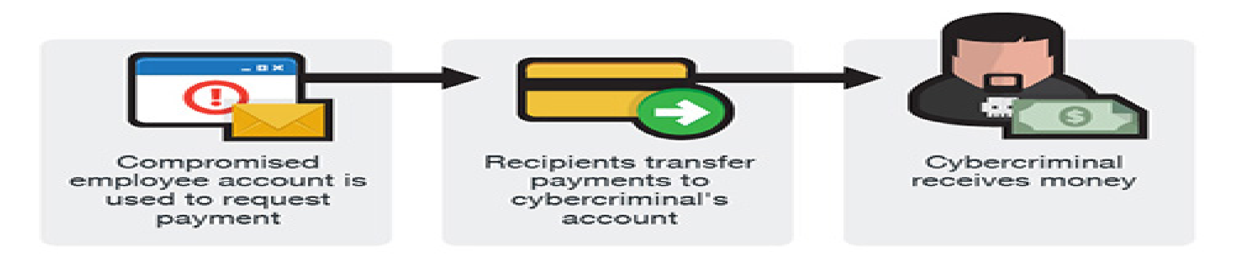
```
Content-Transfer-Encoding: 7bit
Date: Tue, 15 Sep 2015 08:56:11 -0600
From: Tim Rettig <tim.rettig@intrust-it.com>
To: <rebecca.moix@intrust-it.com>
Subject: TRANSFER REQUEST
Reply-To: <ceo.xxl1@aol.com>
Mail-Reply-To: ceo.xxl1@aol.com
```

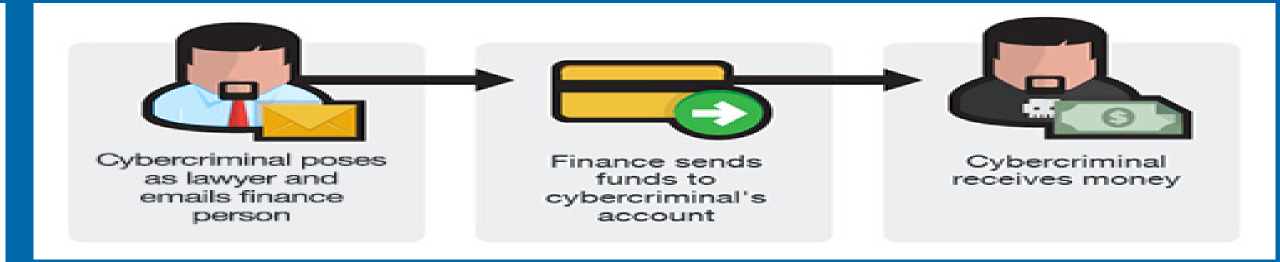
Threats: Business Email Compromise

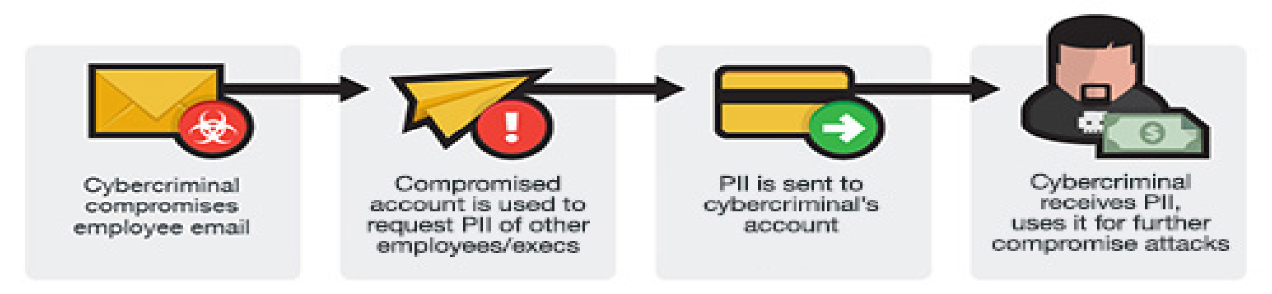
- BEC is an email-based scam where an attacker gains access to one or more email accounts attempting to fool employees into transferring money or sensitive data.


Cybercriminal compromises employee email
Compromised account is used to send notifications to customers
Payments are transferred to cybercriminal's account
Cybercriminal receives money


Cybercriminal poses as company exec and emails finance person
Finance sends funds to cybercriminal's account
Cybercriminal receives money


Compromised employee account is used to request payment
Recipients transfer payments to cybercriminal's account
Cybercriminal receives money


Cybercriminal poses as lawyer and emails finance person
Finance sends funds to cybercriminal's account
Cybercriminal receives money


Cybercriminal compromises employee email
Compromised account is used to request PII of other employees/execs
PII is sent to cybercriminal's account
Cybercriminal receives PII, uses it for further compromise attacks

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes

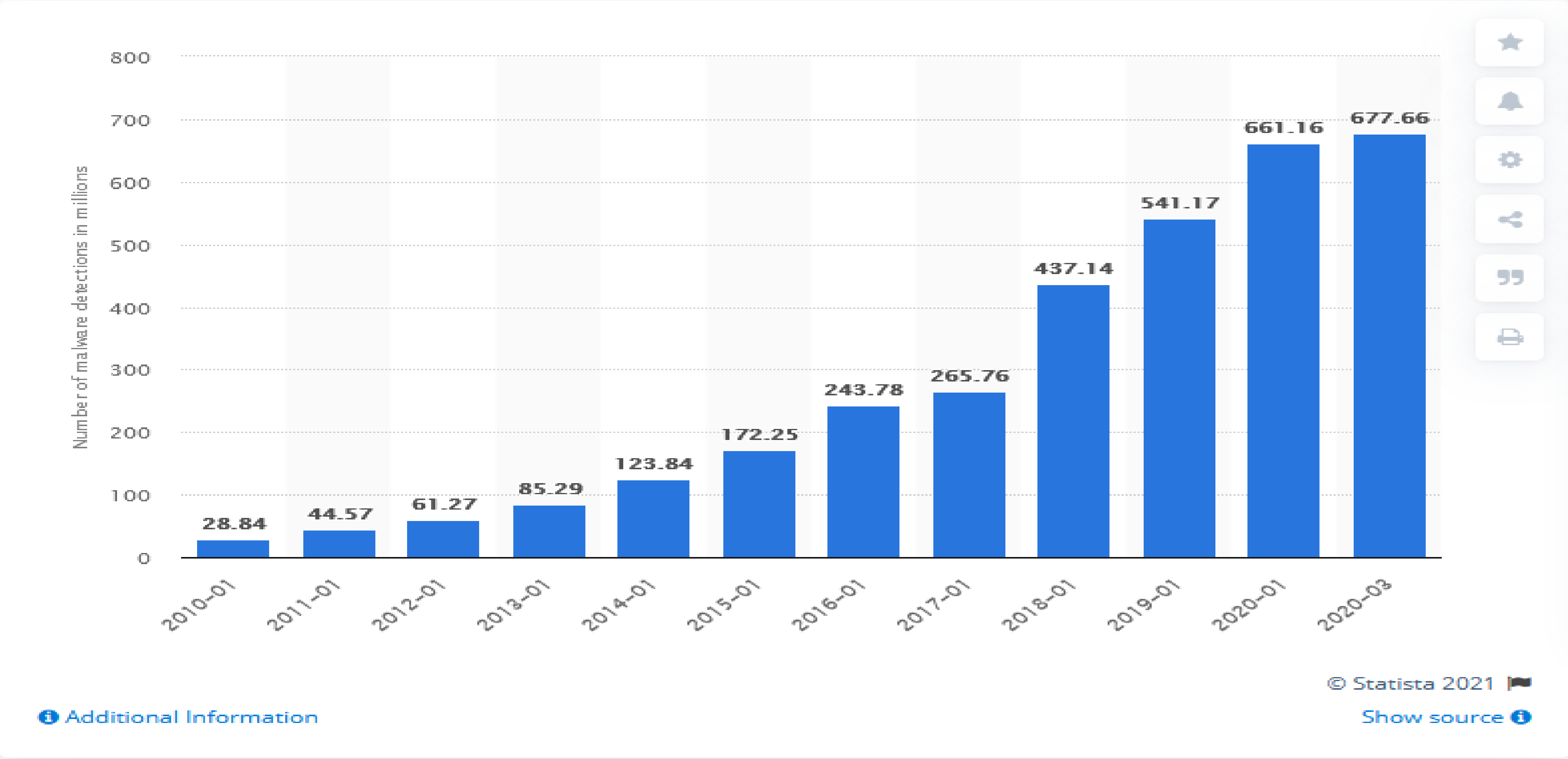
Threats: Real World BEC

- 3 companies impersonated with legitimate business identifiers provided. Email, social media, forms, websites, etc.
- Over a dozen purchased domains that were then registered as email accounts, used, and monitored
- Virtually every phone number provided either was disconnected when called or rang through to a generic voicemail
- Custom designed forms and signatures for all of the businesses and individuals who were being impersonated
- Company addresses, delivery locations, phone numbers, references from all over the country including Florida, Texas, New Jersey, California, Colorado, Indiana, Kentucky

Threats: Malware

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

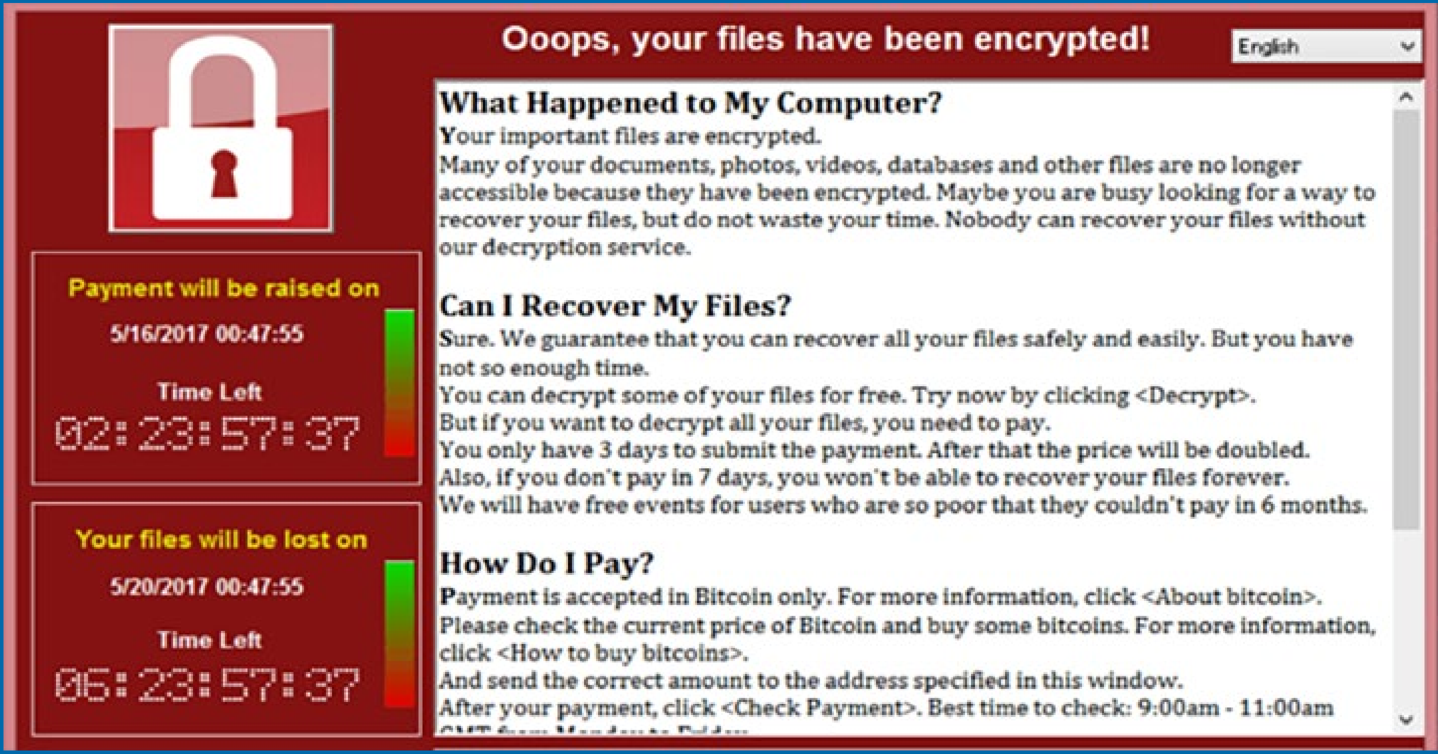
Malware growth



© Statista 2021

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



Ooops, your files have been encrypted!

English

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

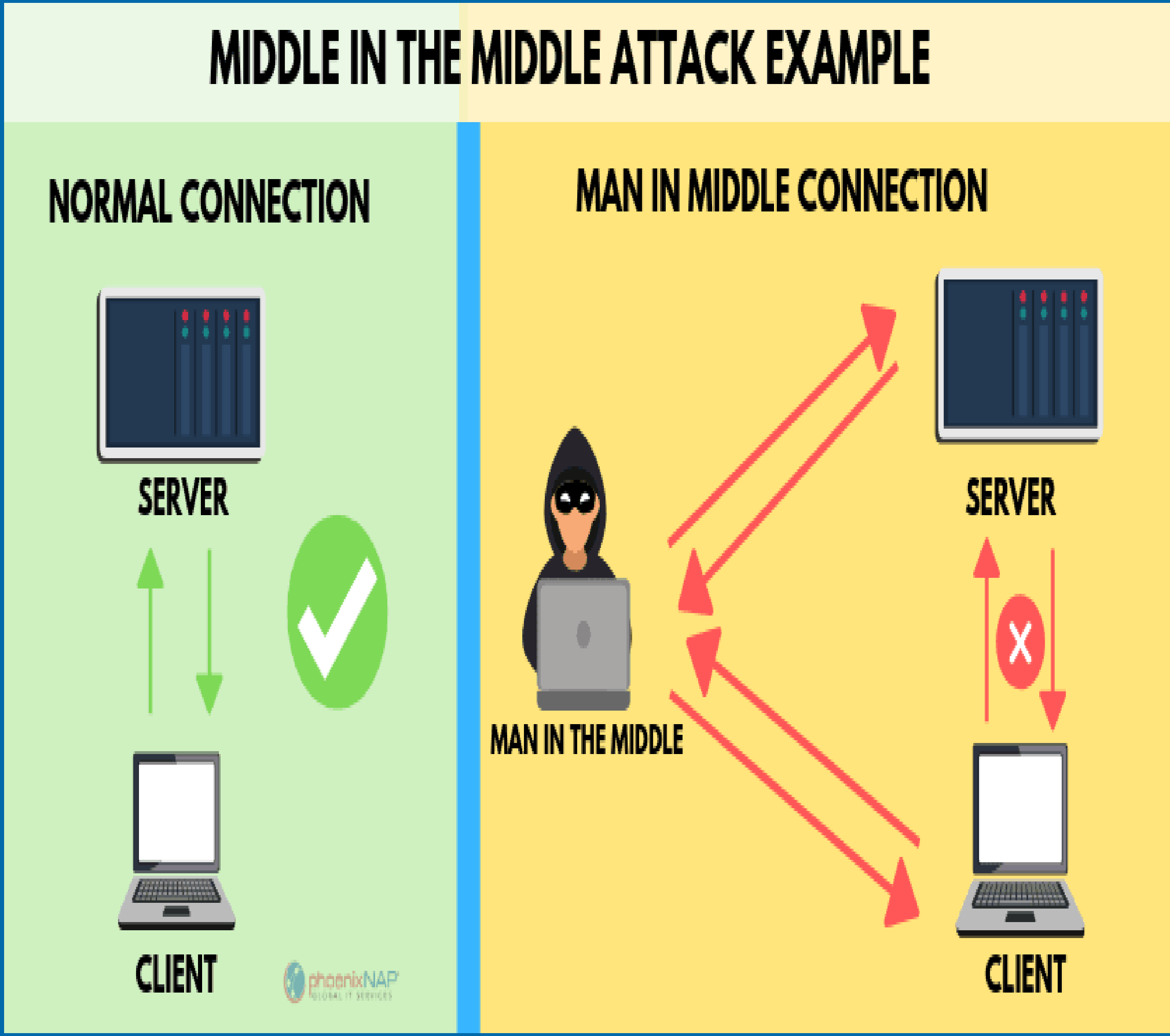
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Threats: Public Wi-Fi

- Information can be stolen
- Malware can be planted

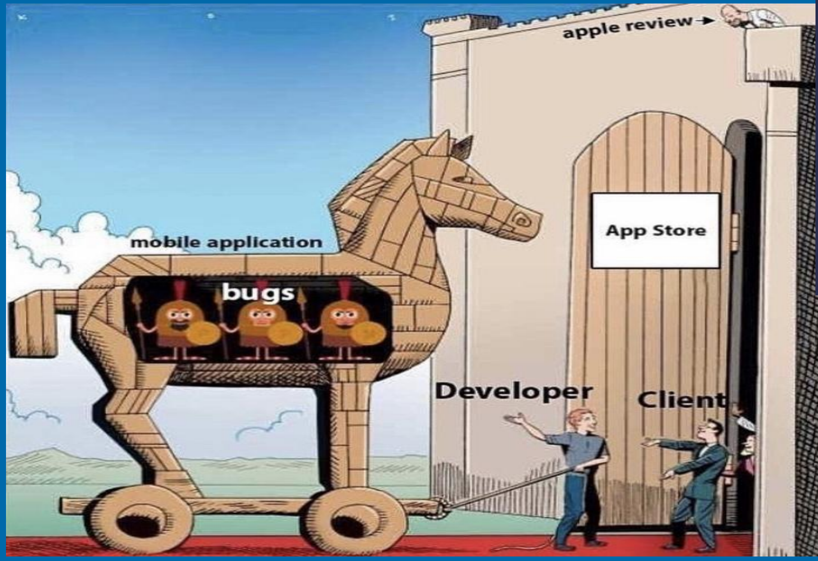
Using Public Wi-Fi in a cyber security conference

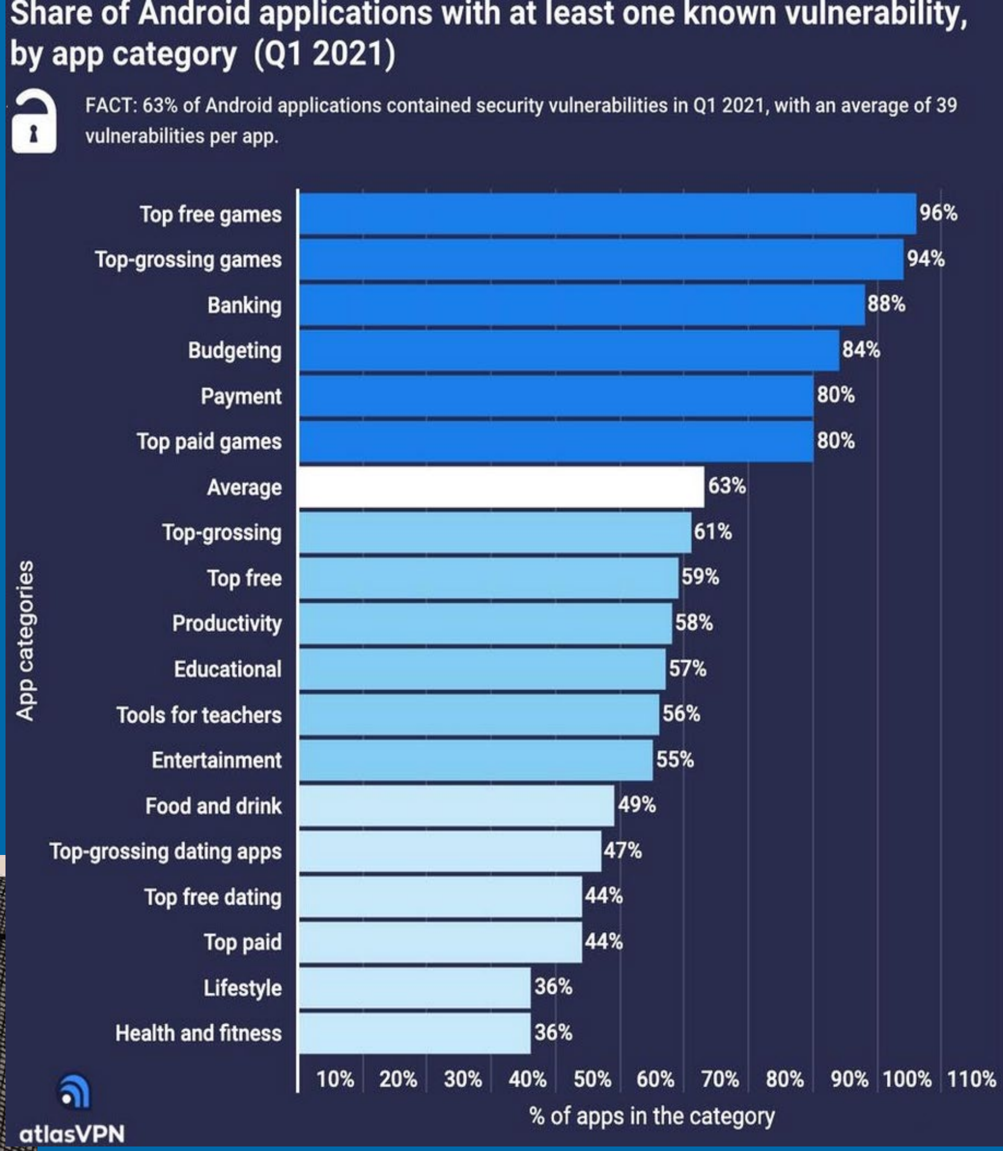


MIDDLE IN THE MIDDLE ATTACK EXAMPLE

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

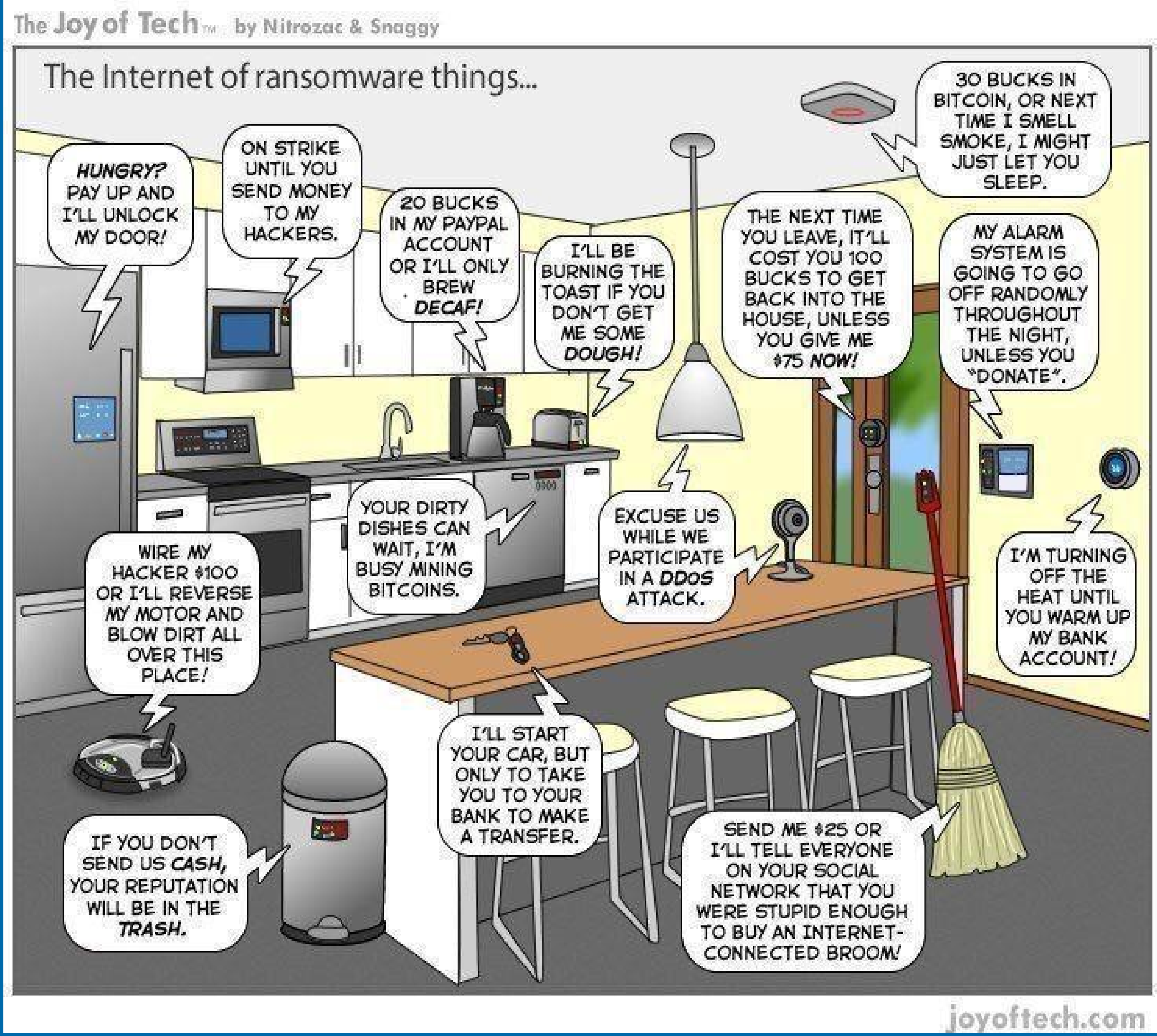
I THINK MY PRIVACY SETTINGS ARE WRONG.
SLANE CARTOONS
SLANE.co.nz
ENSURE YOUR PROFILE IS SECURE ON SOCIAL MEDIA SITES.

Threats: Mobile Devices

- Patching issues
- Misconfiguration
- Apps steal data
- Malware
- Sensitive data loss
- Split tunneling issues

Threats: Internet of Things (IoT)

- 50 billion devices by 2020
- 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

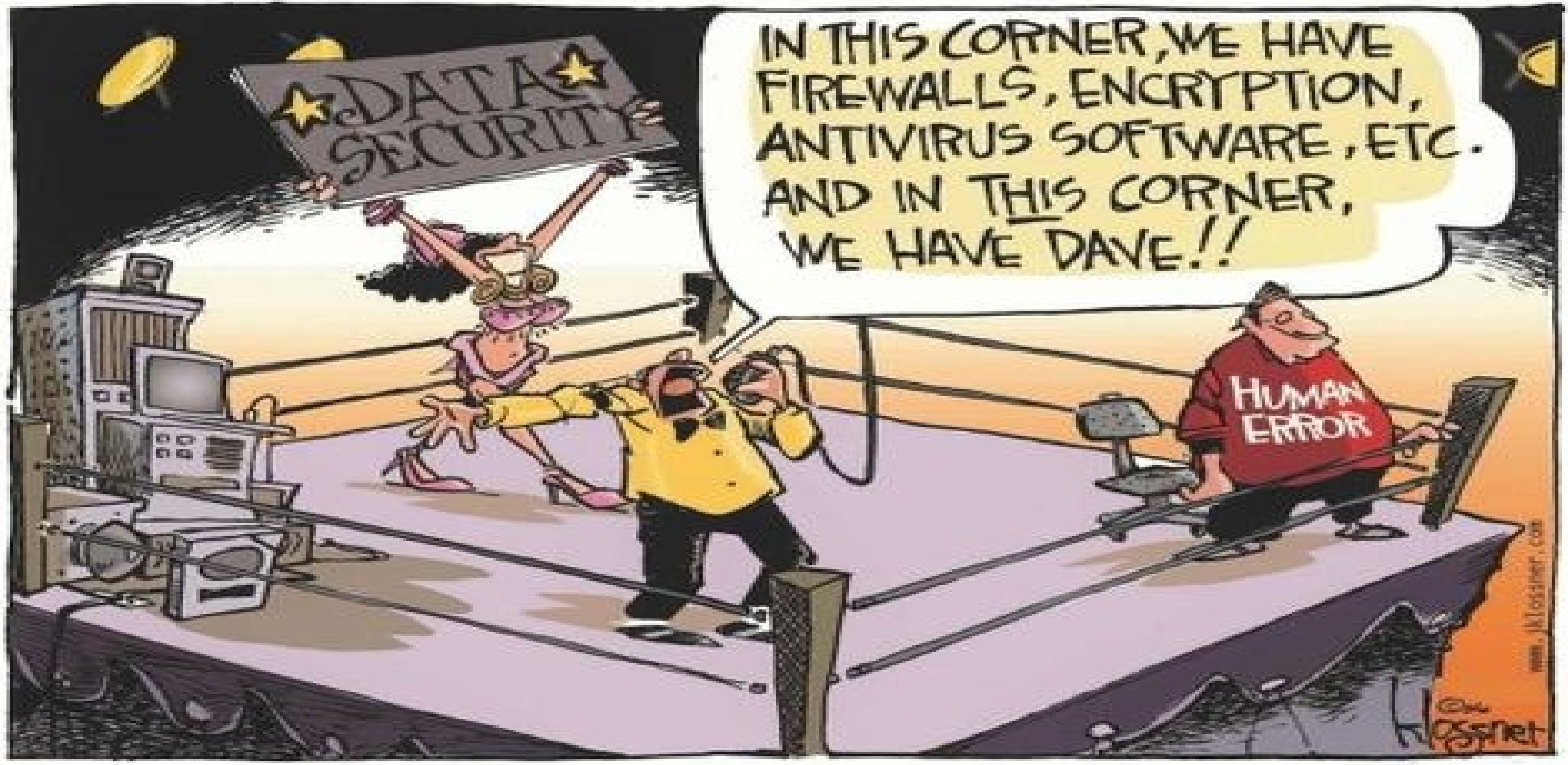

The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
joyoftech.com

Threats: Insider Threats

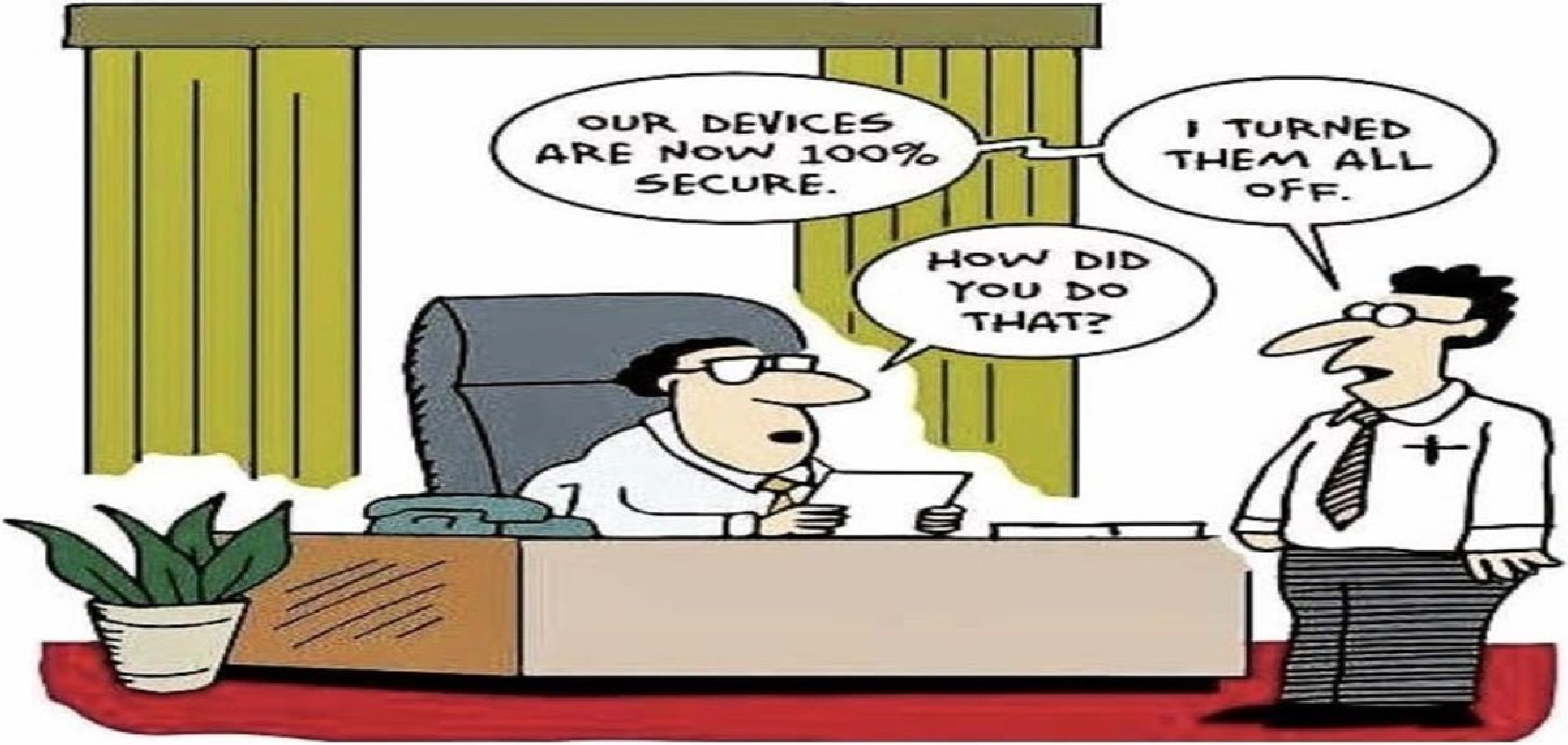
"A malicious insider is an employee or authorized person who uses his data access for harmful, unethical, or illegal activities. Because of the wider access available internally, insiders are often harder to detect and apprehend than external attackers or hackers" – Answers.com

Stockfinland / Getty Images

Don't be a "Dave"


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.JMossner.com
Mossner

Defenses


OUR DEVICES ARE NOW 100% SECURE.
HOW DID YOU DO THAT?
I TURNED THEM ALL OFF.

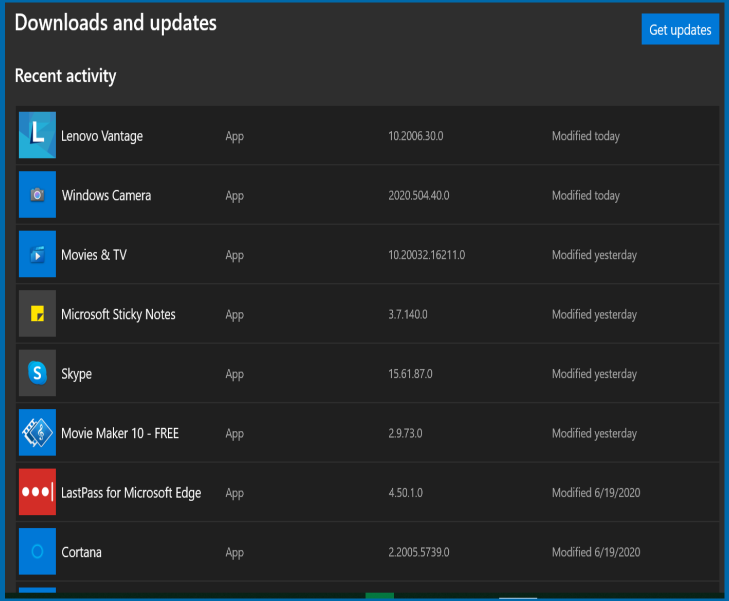
Defenses

It might feel like this…

Don’t be scared be prepared!

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

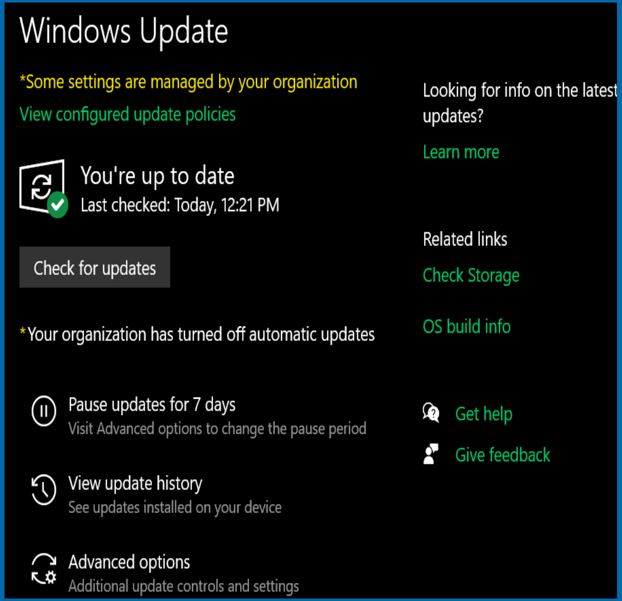


Downloads and updates

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

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

Looking for info on the latest updates?

Learn more

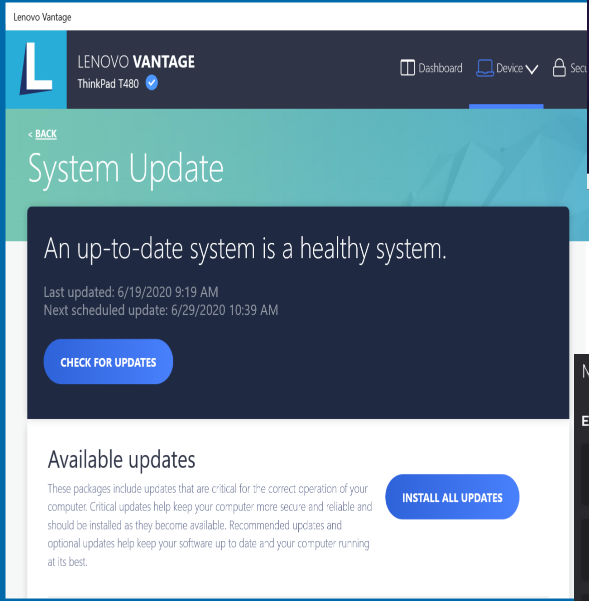
Related links

Check Storage

OS build info

Get help

Give feedback



Lenovo Vantage

LENOVO VANTAGE
ThinkPad T480

< BACK

System Update

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

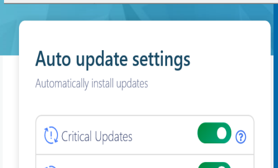
Last updated: 6/19/2020 9:19 AM
Next scheduled update: 6/29/2020 10:39 AM

CHECK FOR UPDATES

Available updates

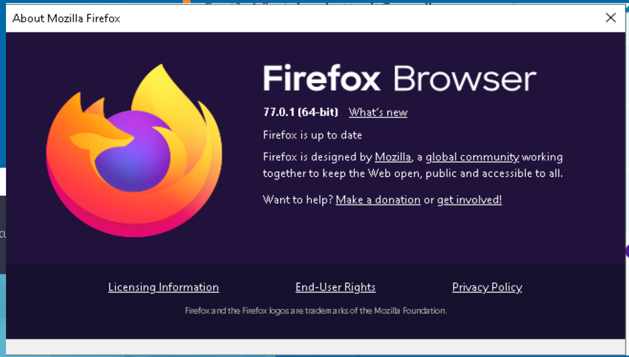
These packages include updates that are critical for the correct operation of your computer. Critical updates help keep your computer more secure and reliable and should be installed as they become available. Recommended updates and optional updates help keep your software up to date and your computer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

INSTALL ALL UPDATES



Auto update settings
Automatically install updates

Critical Updates



About Mozilla Firefox

Firefox Browser

77.0.1 (64-bit) What's new

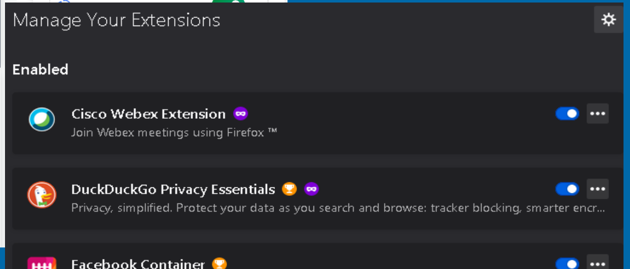
Firefox is up to date

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.



Manage Your Extensions

Enabled

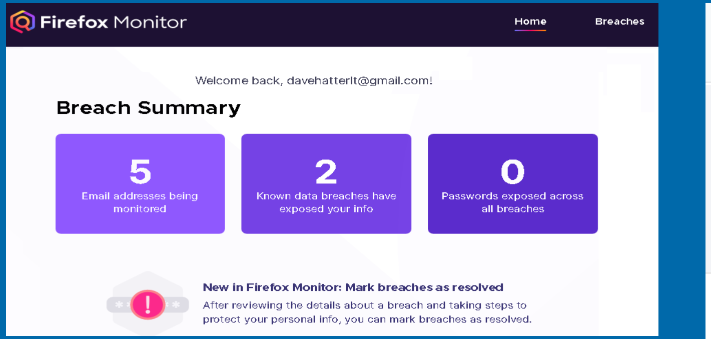
Cisco Webex Extension
Join Webex meetings using Firefox ™

DuckDuckGo Privacy Essentials
Privacy, simplified. Protect your data as you search and browse: tracker blocking, smarter encr...

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



Welcome back, davehatterlt@gmail.com!

Breach Summary

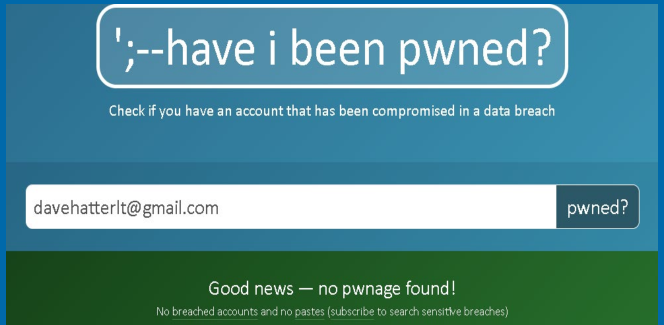
5 Email addresses being monitored

2 Known data breaches have exposed your info

0 Passwords exposed across all breaches

New in Firefox Monitor: Mark breaches as resolved

After reviewing the details about a breach and taking steps to protect your personal info, you can mark breaches as resolved.

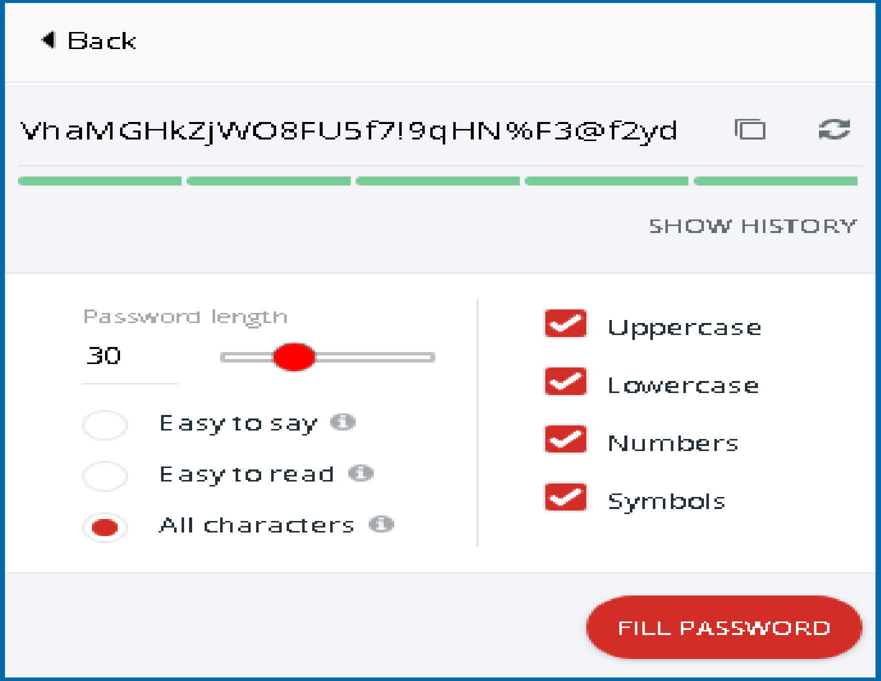


Check if you have an account that has been compromised in a data breach

davehatterlt@gmail.com

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)



VhaMGHkZjWO8FU5f7!9qHN%F3@f2yd

Password length 30

○ Easy to say

○ Easy to read

● All characters

☑ Uppercase

☑ Lowercase

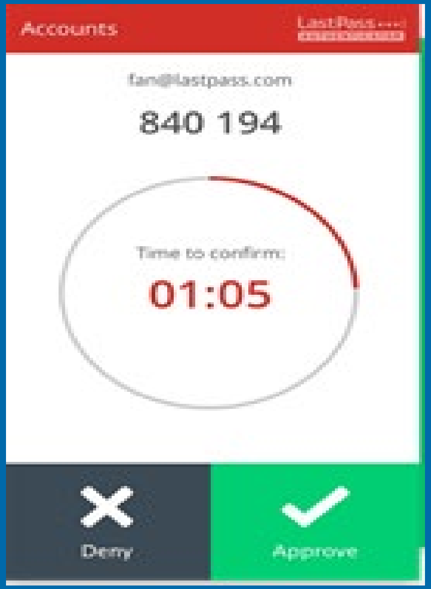
☑ Numbers

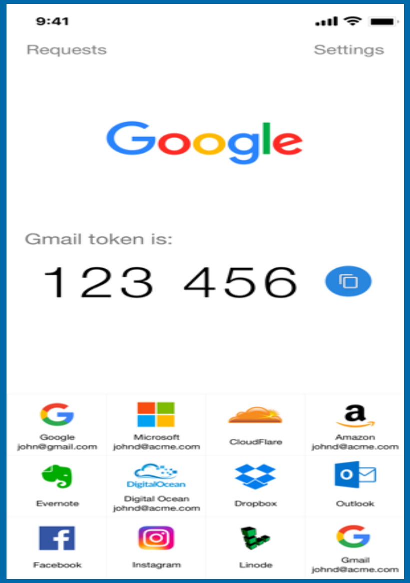
☑ Symbols

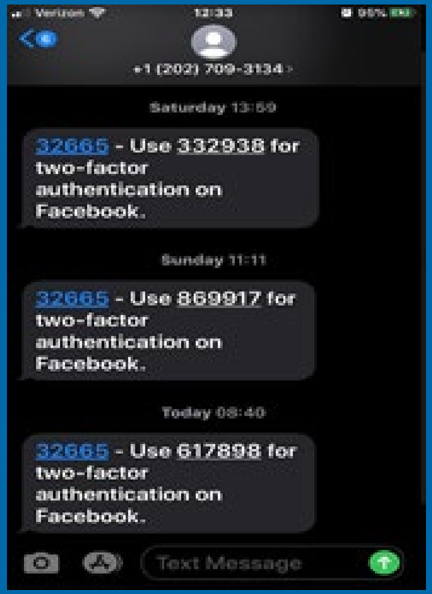
- ✗ Previous breach exposures
- ✗ Less than 8 characters
- ✗ Context-specific words
- ✗ Dictionary words
- ✗ Repetitive characters
- ✗ Password hints

Defenses: Multi-factor Authentication

- MFA: Aka Two-factor Authentication 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 like Authy rather than SMS based OTPs







Saturday 13:59

32665 - Use 332938 for two-factor authentication on Facebook.

Sunday 11:11

32665 - Use 869917 for two-factor authentication on Facebook.

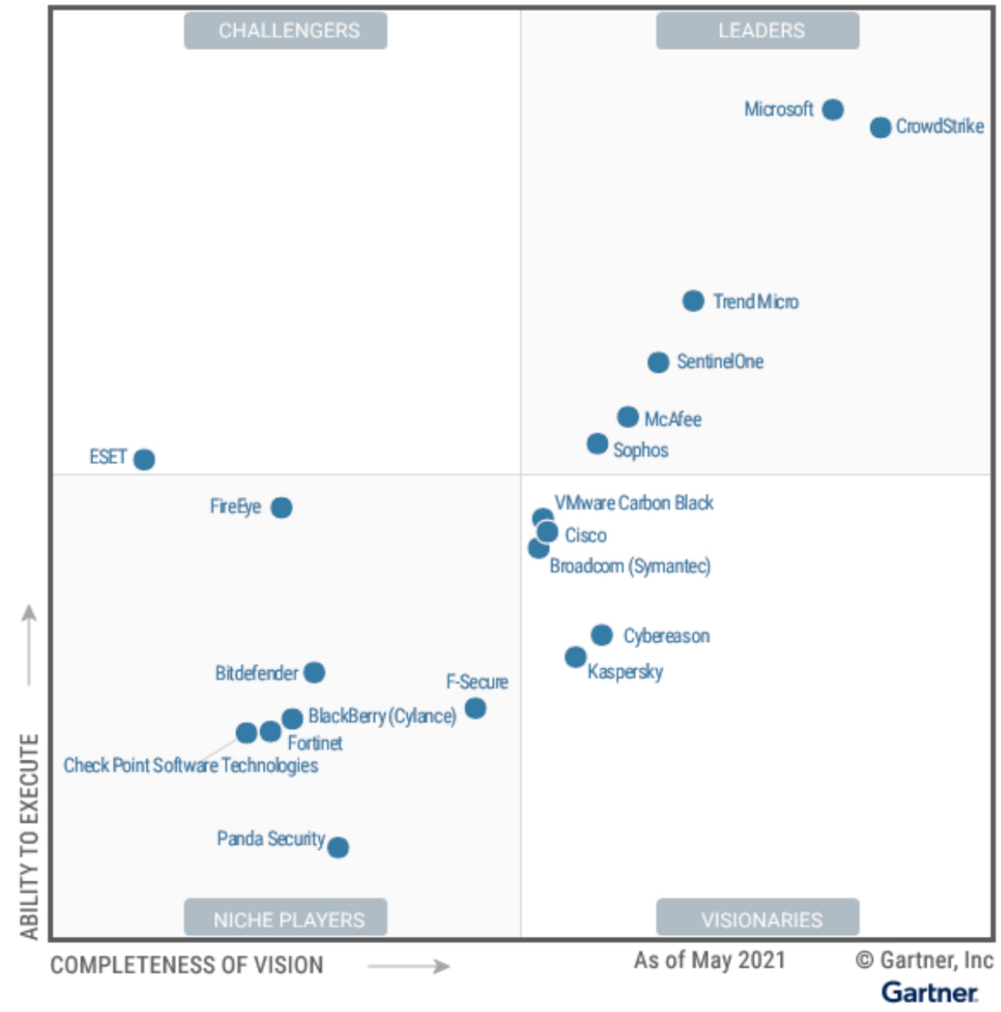
Today 08:40

32665 - Use 617898 for two-factor authentication on Facebook.

"I'M YOUR HUSBAND, I DIDN'T THINK I NEEDED TO USE MULTIFACTOR AUTHENTICATION."

Defenses: Endpoint Protection

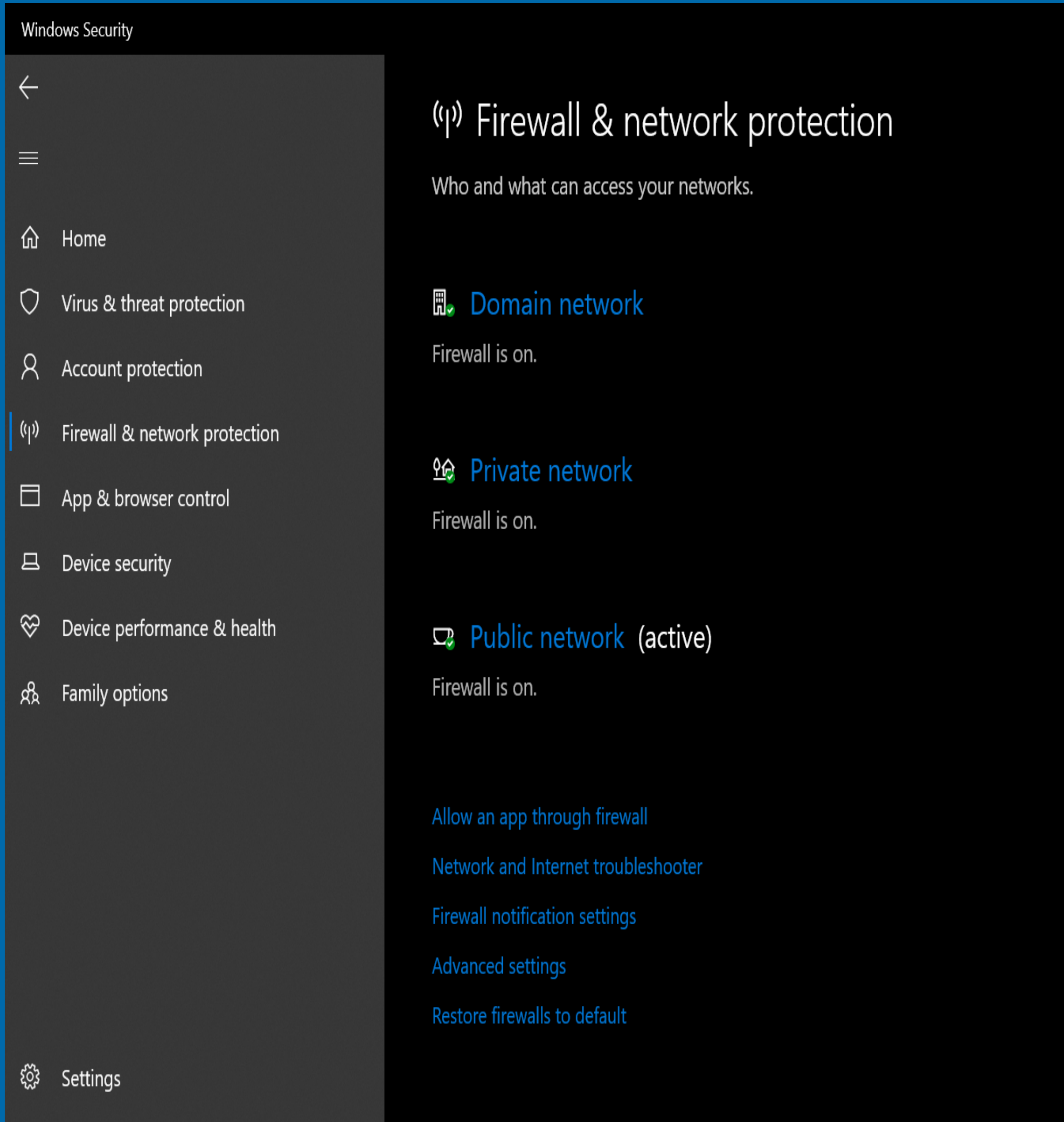
- Vendors regularly release updates
- Also known as anti-malware or anti-virus software
- Update definitions
- Disable everything and enable functionality as required
- Consider more than one



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


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings

Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

Firewall is on.

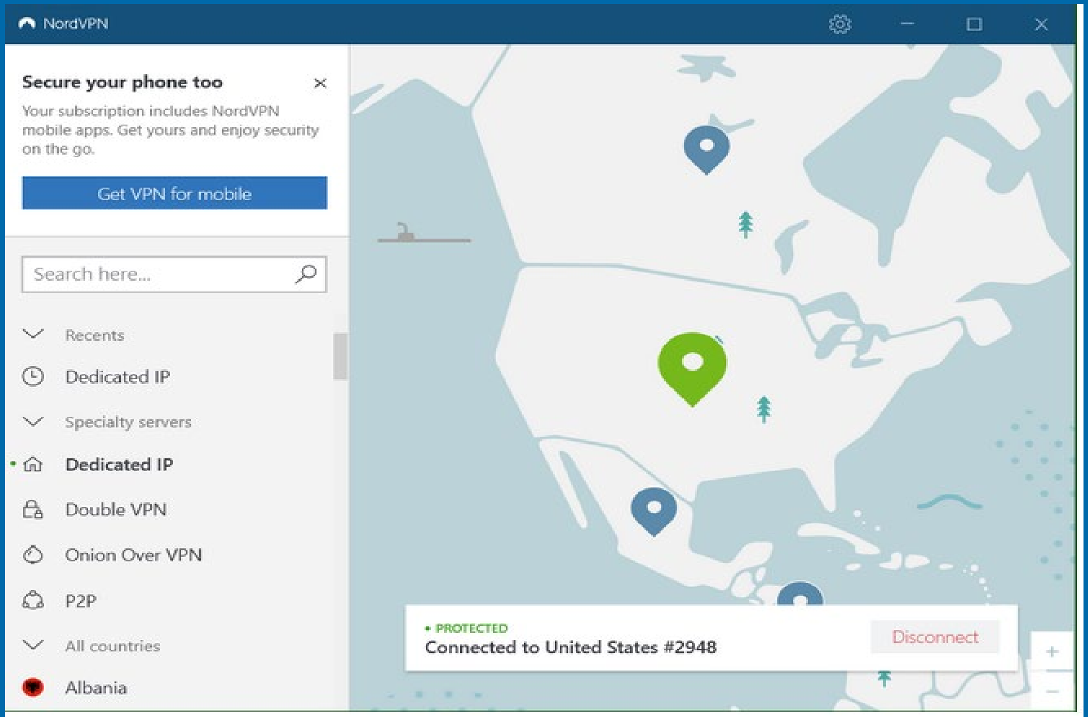
Public network (active)

Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

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!

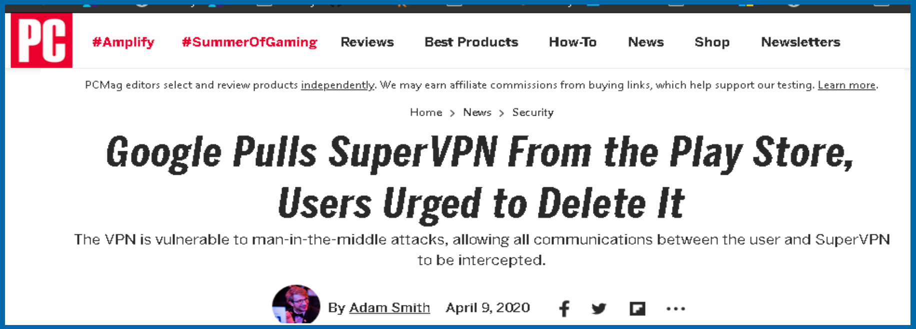


Secure your phone too

Your subscription includes NordVPN mobile apps. Get yours and enjoy security on the go.

Get VPN for mobile

• PROTECTED
Connected to United States #2948



PCMag editors select and review products independently. We may earn affiliate commissions from buying links, which help support our testing. Learn more.

Home > News > Security

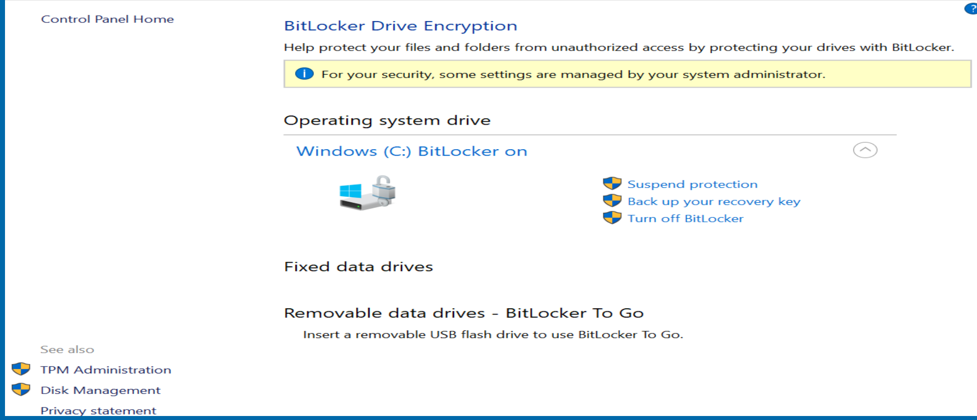
Google Pulls SuperVPN From the Play Store, Users Urged to Delete It

The VPN is vulnerable to man-in-the-middle attacks, allowing all communications between the user and SuperVPN to be intercepted.

By Adam Smith April 9, 2020

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 a rest
- Look for https:// in the browser
- Use encryption to protect email
- Use encryption to protect messaging



Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

Windows (C:) BitLocker on

Suspend protection
Back up your recovery key
Turn off BitLocker

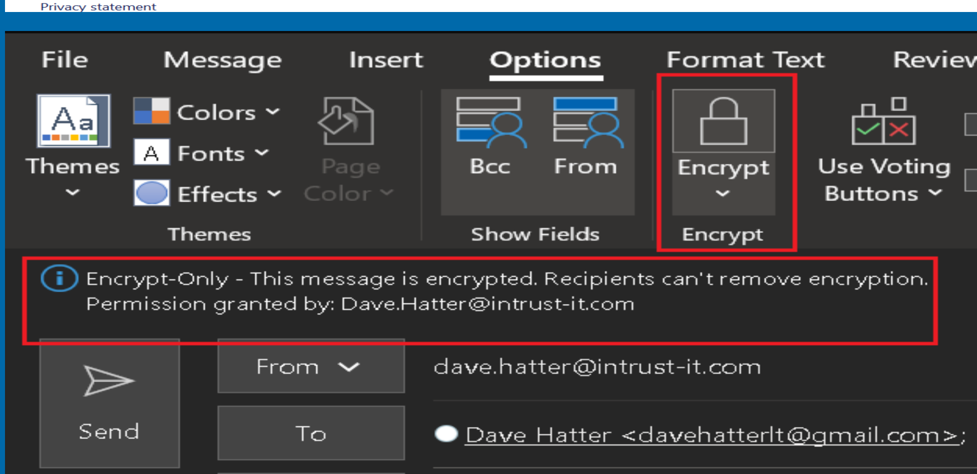
Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

See also

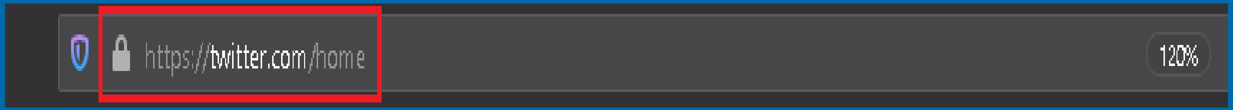
TPM Administration
Disk Management
Privacy statement



Encrypt-Only - This message is encrypted. Recipients can't remove encryption.
Permission granted by: Dave.Hatter@intrust-it.com

From dave.hatter@intrust-it.com

To Dave Hatter <davehatterlt@gmail.com>;

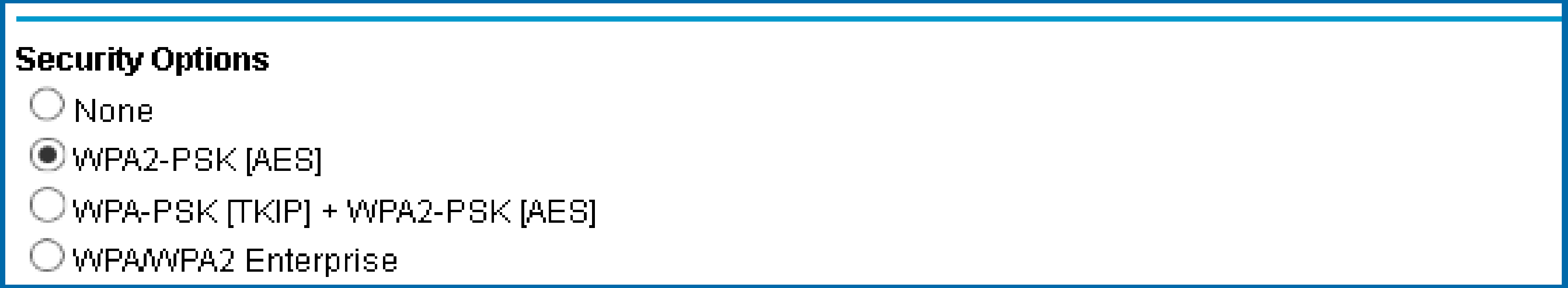


https://twitter.com/home

120%

Defenses: Router

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



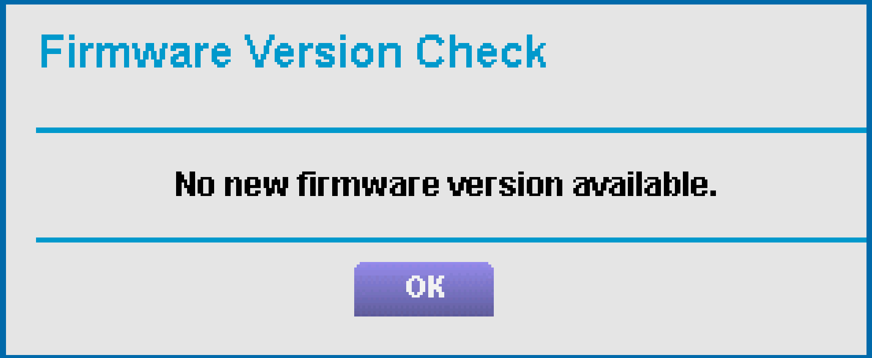
Security Options

○ None

● WPA2-PSK [AES]

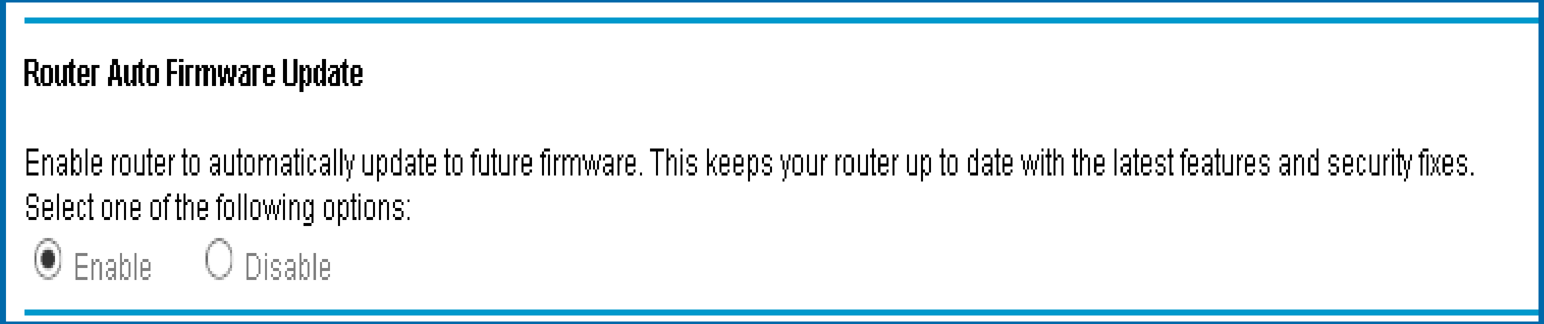
○ WPA-PSK [TKIP] + WPA2-PSK [AES]

○ WPA/WPA2 Enterprise



Firmware Version Check

No new firmware version available.



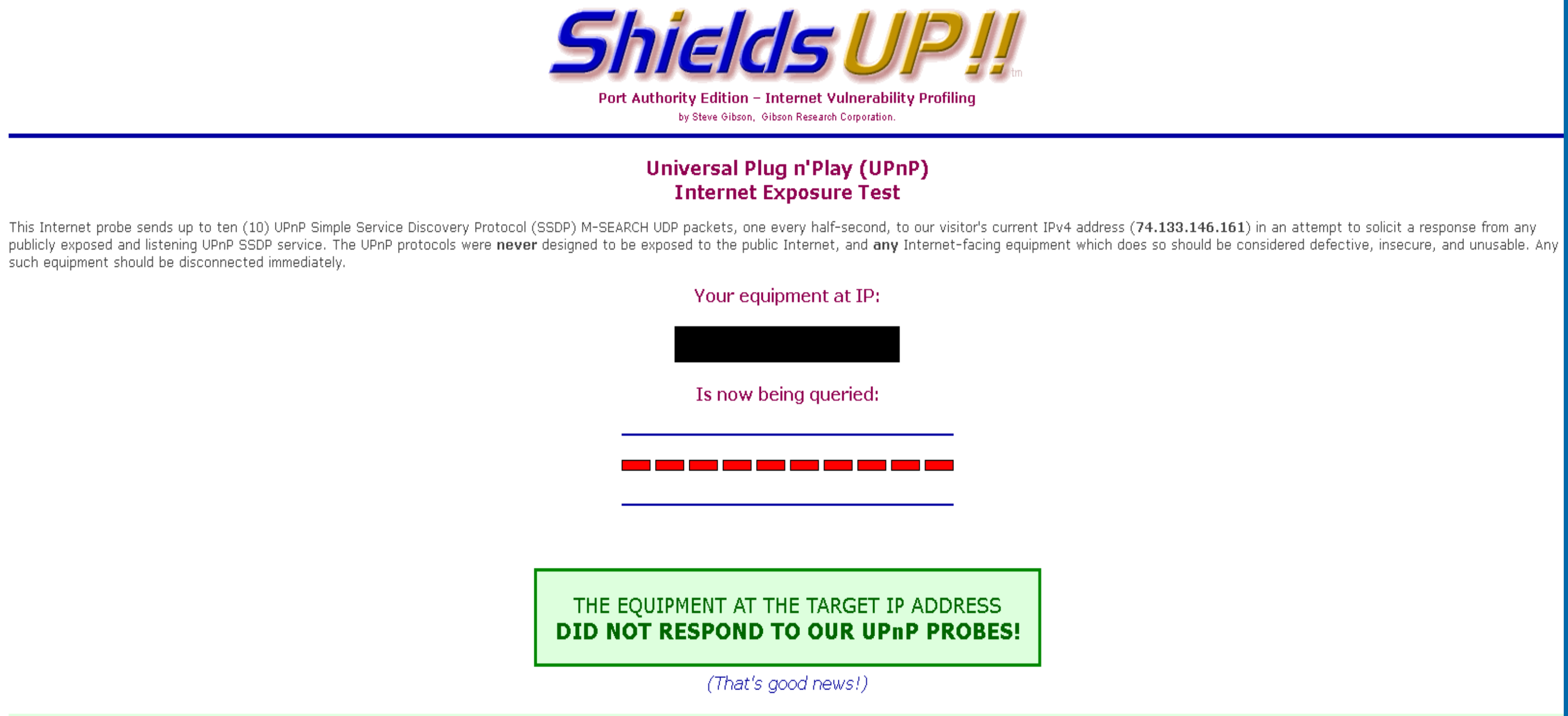
Router Auto Firmware Update

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

Defenses: Router

- Disable SSID broadcast
- Whitelist devices
- Disable WPS
- Use 3rd party DNS
- Disable remote management
- Create VLANS



Shields UP!!

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

Universal Plug n'Play (UPnP)
Internet Exposure Test

This Internet probe sends up to ten (10) UPnP Simple Service Discovery Protocol (SSDP) M-SEARCH UDP packets, one every half-second, to our visitor's current IPv4 address (**74.133.146.161**) in an attempt to solicit a response from any publicly exposed and listening UPnP SSDP service. The UPnP protocols were **never** designed to be exposed to the public Internet, and **any** Internet-facing equipment which does so should be considered defective, insecure, and unusable. Any such equipment should be disconnected immediately.

Your equipment at IP:

[redacted]

Is now being queried:

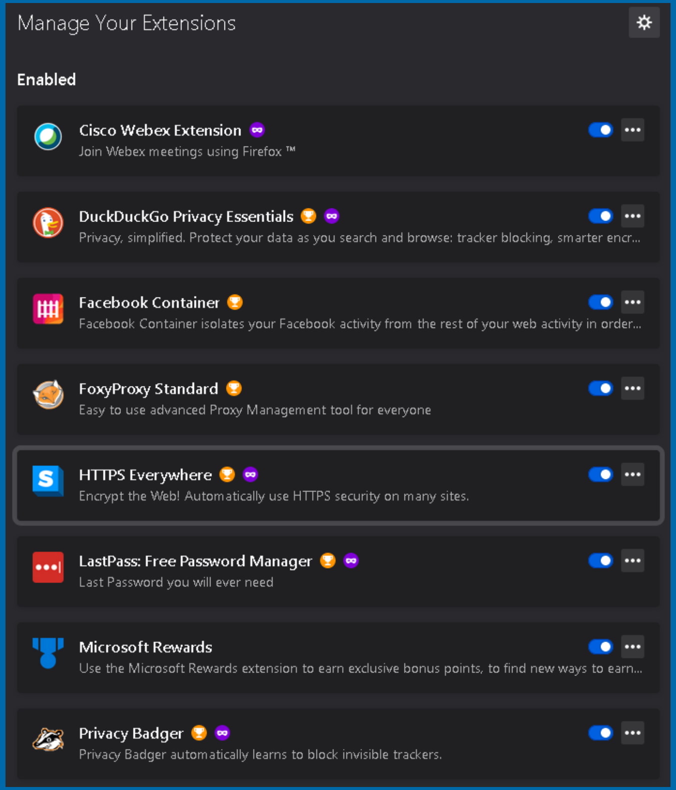
THE EQUIPMENT AT THE TARGET IP ADDRESS
DID NOT RESPOND TO OUR UPnP PROBES!

(That's good news!)

https://www.grc.com/shieldsup

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



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 encr...

Facebook Container
Facebook Container isolates your Facebook activity from the rest of your web activity in order...

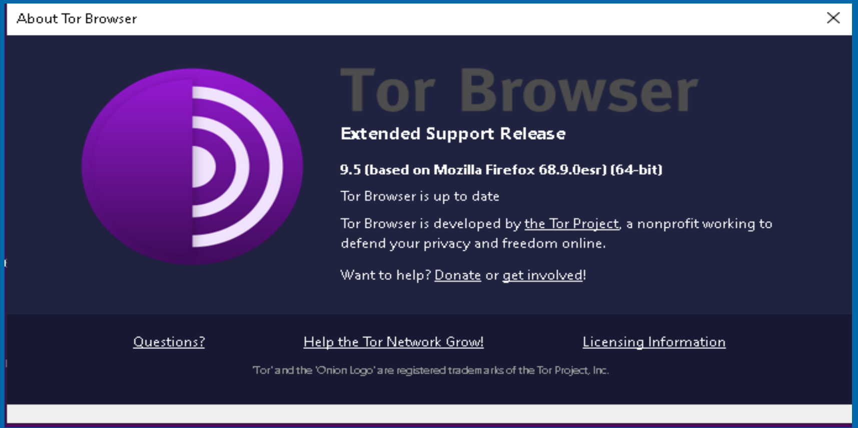
FoxyProxy Standard
Easy to use advanced Proxy Management tool for everyone

HTTPS Everywhere
Encrypt the Web! Automatically use HTTPS security on many sites.

LastPass: Free Password Manager
Last Password you will ever need

Microsoft Rewards
Use the Microsoft Rewards extension to earn exclusive bonus points, to find new ways to earn...

Privacy Badger
Privacy Badger automatically learns to block invisible trackers.



About Tor Browser

Tor Browser

Extended Support Release

9.5 (based on Mozilla Firefox 68.9.0esr) (64-bit)

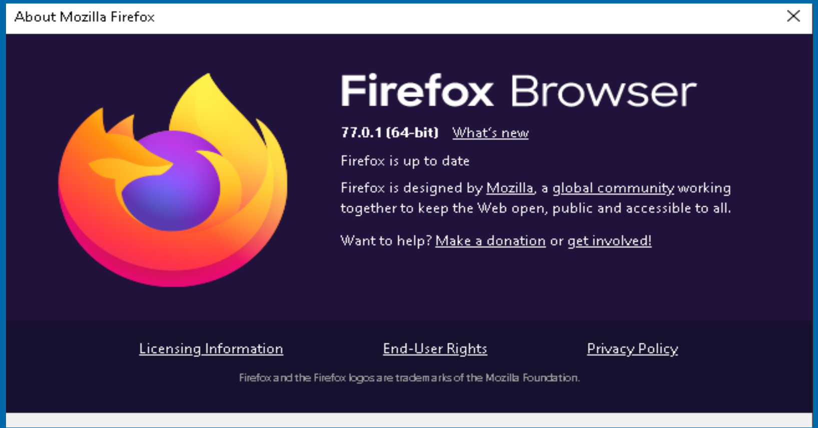
Tor Browser is up to date

Tor Browser is developed by the Tor Project, a nonprofit working to defend your privacy and freedom online.

Want to help? Donate or get involved!

Questions? Help the Tor Network Grow! Licensing Information

'Tor' and the 'Onion Logo' are registered trademarks of the Tor Project, Inc.



About Mozilla Firefox

Firefox Browser

77.0.1 (64-bit) What's new

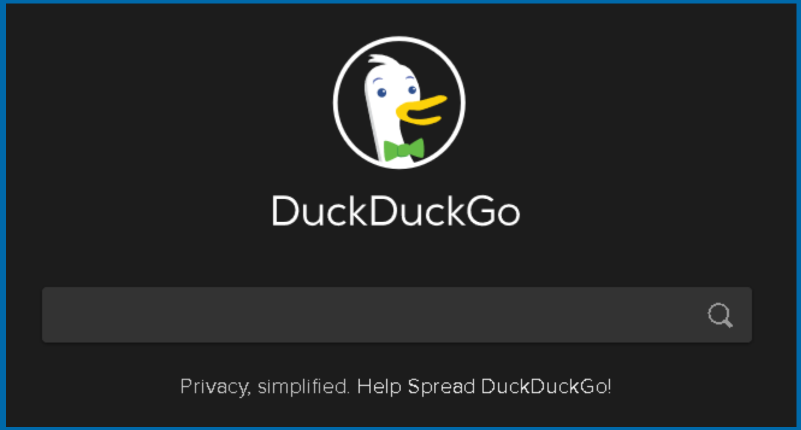
Firefox is up to date

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.

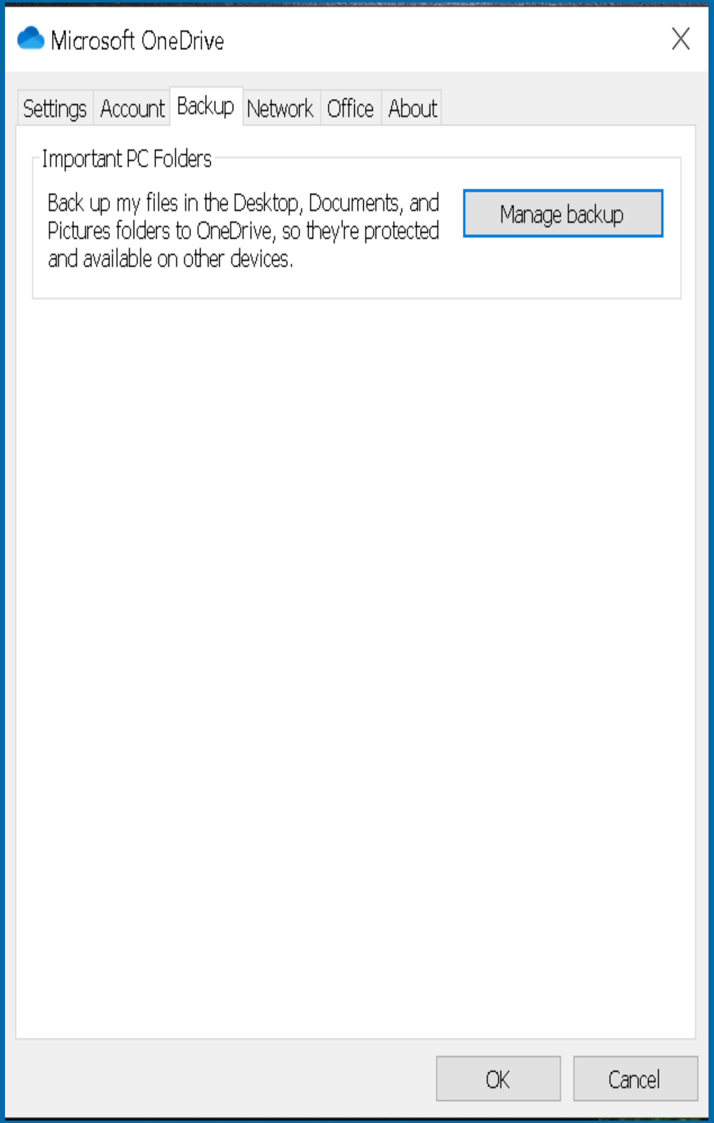


DuckDuckGo

Privacy, simplified. Help Spread DuckDuckGo!

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



Important PC Folders

Back up my files in the Desktop, Documents, and Pictures folders to OneDrive, so they're protected and available on other devices.

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

lome • CIS Benchmarks

CIS Benchmarks™

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.

Overview of CIS Benchmarks and CIS-CAT Demo

Register for the Webinar
Tues. June 23 at 10:00 AM EDT
Tues. July 7 at 1:30 PM EDT

CIS Benchmarks FAQ

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 Darkweb 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: General

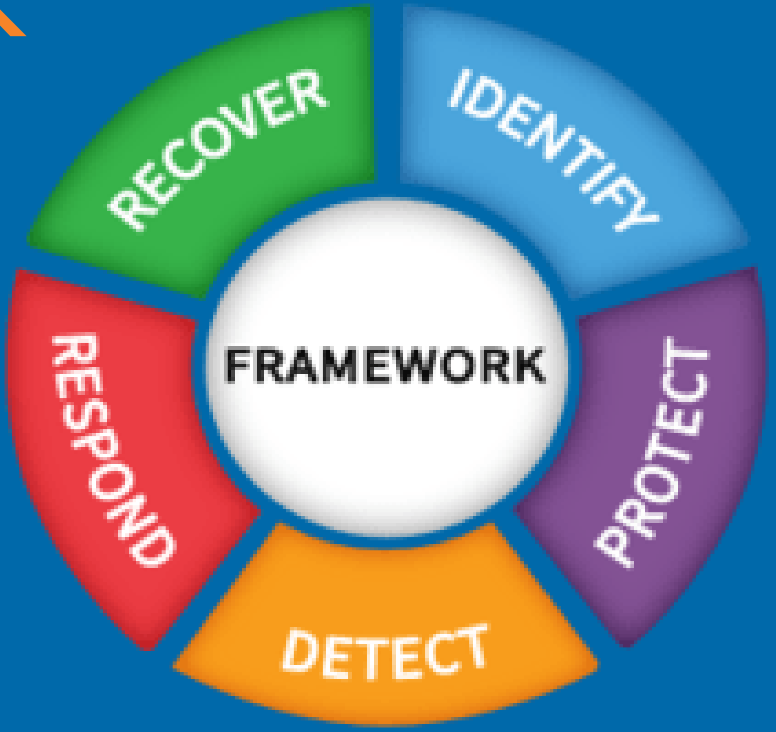
- Prioritize risk
- Be wary of remote access
- Sanitize old equipment
- Maintain a clean desk policy
- Vendor management
- Disable devices that can watch/listen while working
- Don’t allow family to use work devices
- Keep work data on work devices only

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

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
- CIS Controls V8 just published



CIS Center for Internet Security®
Confidence in the Connected World®

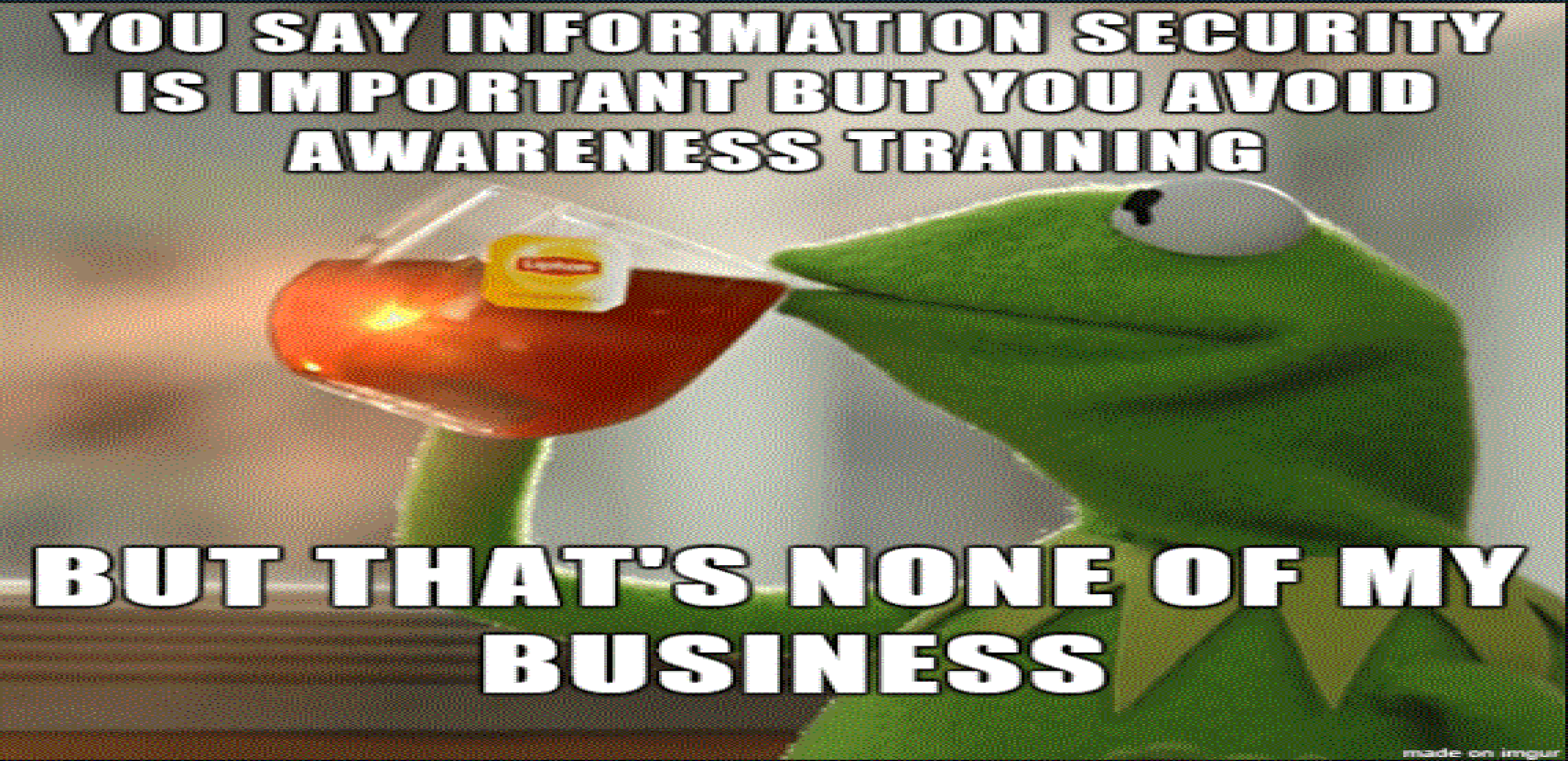
CIS Controls

CIS Controls Version 8

Tools

- Microsoft Defender / Sentinel One
- Open DNS
- BitLocker
- AppLocker
- LastPass
- KnowBe4
- Azure Sentinel / Perch
- Duo
- Nessus

Be vigilant and keep learning!


YOU SAY INFORMATION SECURITY IS IMPORTANT BUT YOU AVOID AWARENESS TRAINING
BUT THAT'S NONE OF MY BUSINESS
made on imgur

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 requires a huge financial investment
- Cyber breaches are covered by general liability insurance
- Cybersecurity is an IT issue

Hope and denial are NOT a strategy!

Remember the 3 simple steps

- Stop
- Think
- Protect – Be a human firewall

Skepticism and Security

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.mcaffee.com
- www.symantec.com
- www.twofactorauth.org
- www.safer-networking.org
- www.zonealarm.com
- www.webopedia.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.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
- enterprise.verizon.com/resources/reports/dbir/
- www.sans.org/critical-security-controls/
- https://www.us-cert.gov/ncas/current-activity/2019/11/06/cisa-launches-cyber-essentials-small-businesses-and-small-sltt
- www.nist.gov/cyberframework
- https://www.cisecurity.org/blog/cyber-hygiene-guidance-for-windows-10/
- www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- https://www.pcmag.com/roundup/256703/the-best-antivirus-protection
- https://www.pcmag.com/roundup/296955/the-best-vpn-services
- https://www.zdnet.com
- http://www.cnet.com

Q & A

“It’s time for a cybersecurity zeitgeist in the West where cyber hygiene is a meme that is aggressively distributed by those who have mastered it and encouraged to be imitated by those who have experienced it.” - James Scott intrust IT

THANK YOU!

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

Intrust IT

linkedin.com/in/davehatter

twitter.com/davehatter

www.youtube.com/user/davidlhatter

Catch my Tech Friday spot live on 55KRC at 6:30 AM every Friday on 550 AM or http://www.55krc.com