intrust IT

CYBERSECURITY

NOT JUST FOR IT ANYMORE!

Dave Hatter, CISSP, CISA, CISM, CCSP, CSSLP, PMP, ITIL

Cybersecurity Consultant

Intrust IT

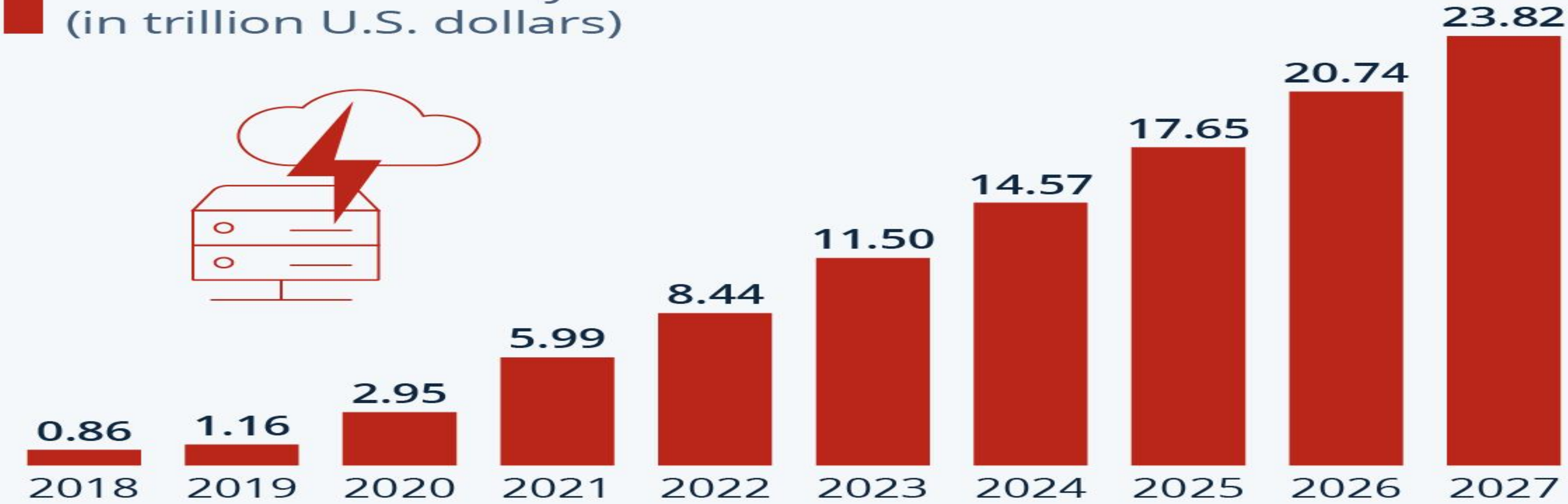
linkedin.com/in/davehatter
twitter.com/davehatter

Agenda

- Where are we?
- Why is this happening now?
- Threats
- Defenses
- Q&A

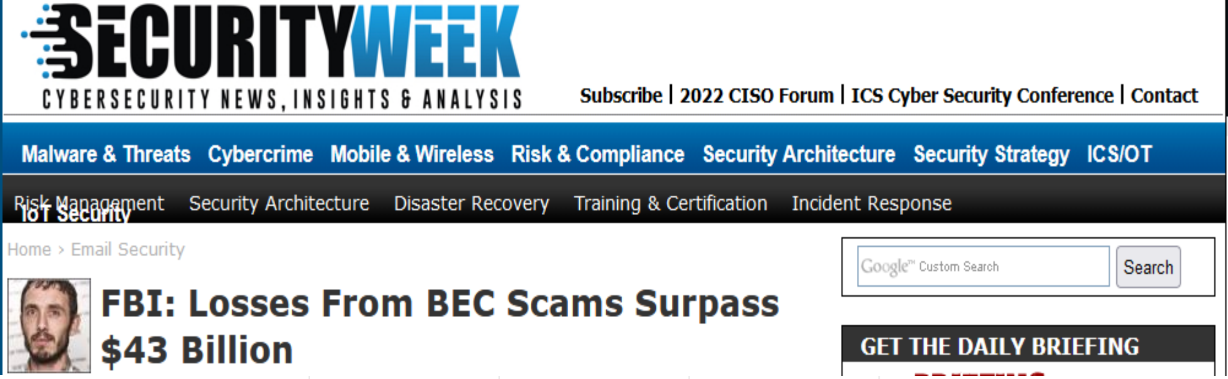
Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)

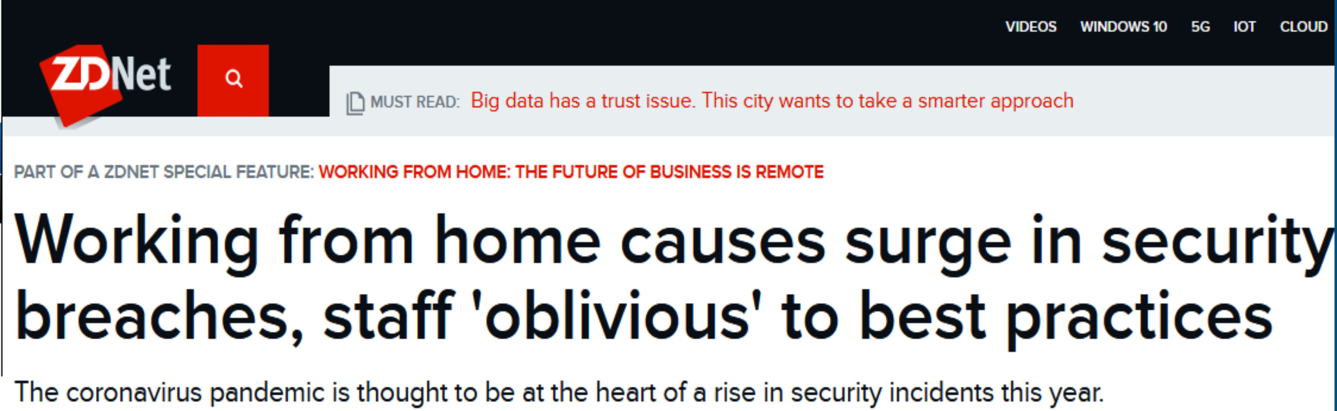


As of November 2022. Data shown is using current exchange rates.

Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF


SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS
Subscribe | 2022 CISO Forum | ICS Cyber Security Conference | Contact
Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Security Strategy ICS/OT
Risk Management Security Architecture Disaster Recovery Training & Certification Incident Response
IoT Security
Home › Email Security
Google Custom Search
Search
GET THE DAILY BRIEFING

FBI: Losses From BEC Scams Surpass $43 Billion

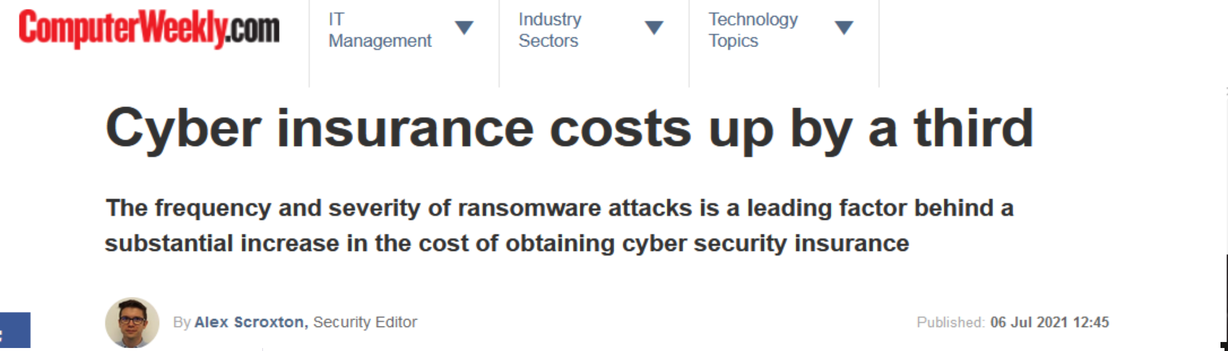


Big data has a trust issue. This city wants to take a smarter approach

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.

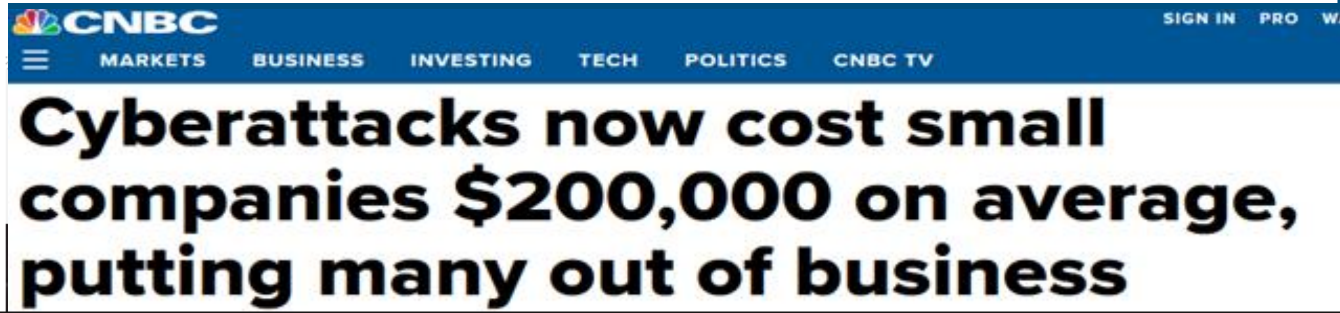


Cyber insurance costs up by a third

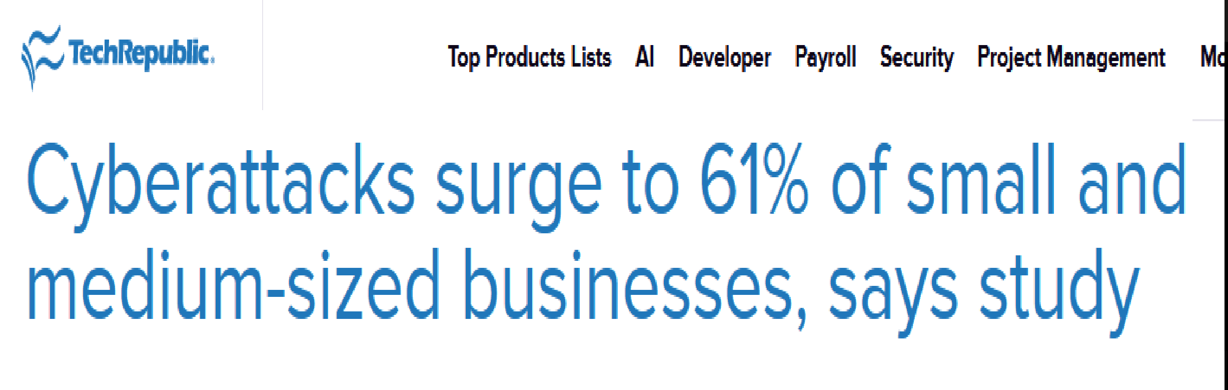
The frequency and severity of ransomware attacks is a leading factor behind a substantial increase in the cost of obtaining cyber security insurance

By Alex Scroxton, Security Editor

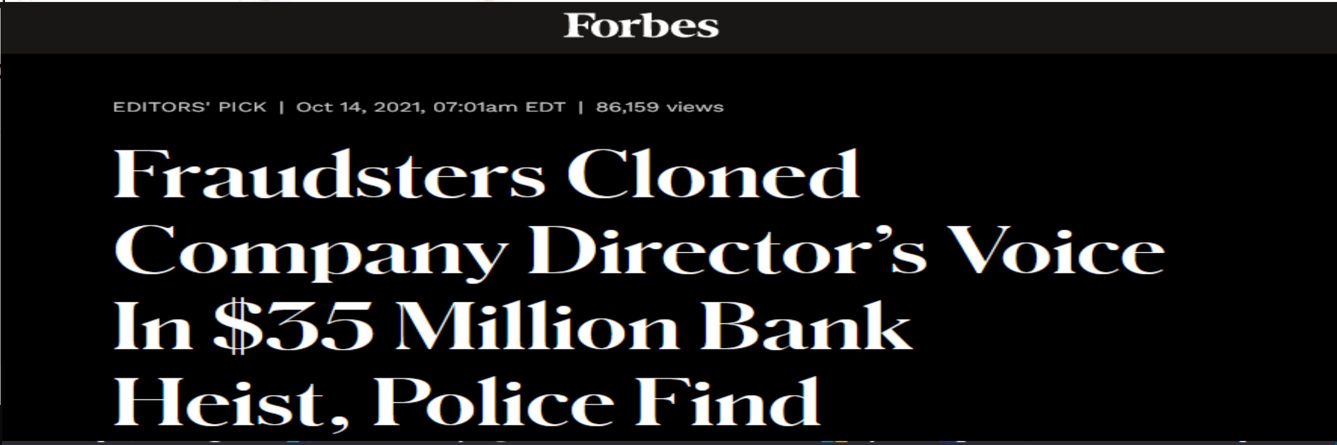
Published: 06 Jul 2021 12:45



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

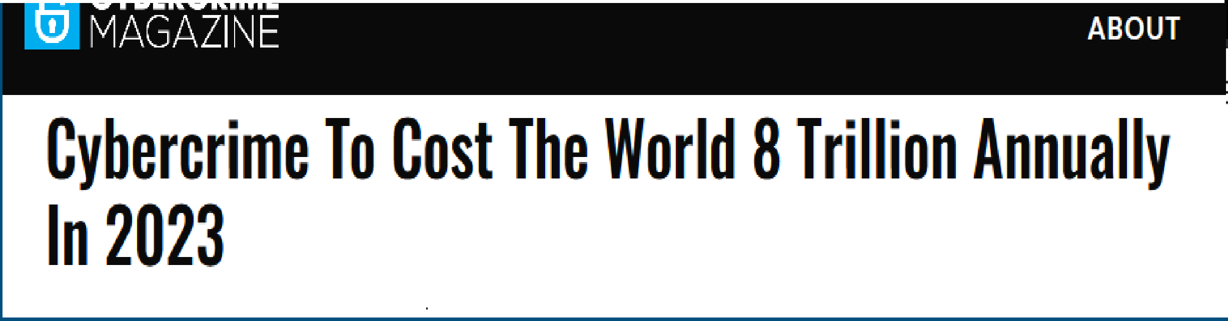

TechRepublic.
Top Products Lists AI Developer Payroll Security Project Management

Cyberattacks surge to 61% of small and medium-sized businesses, says study

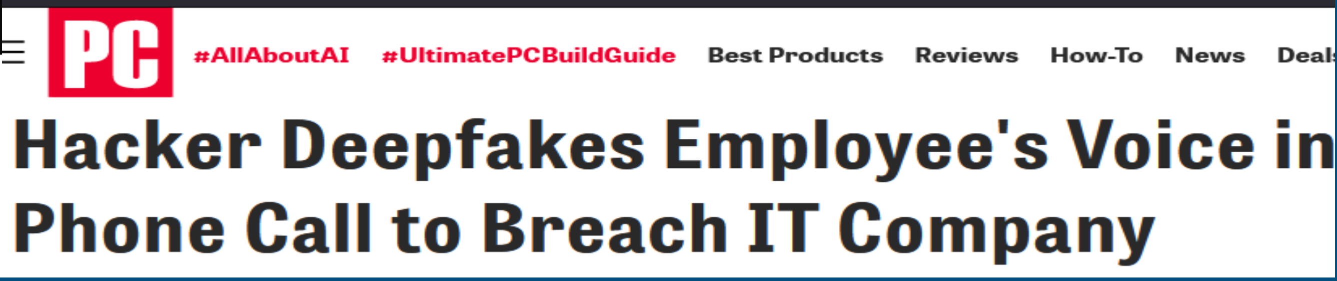


EDITORS' PICK | Oct 14, 2021, 07:01am EDT | 86,159 views

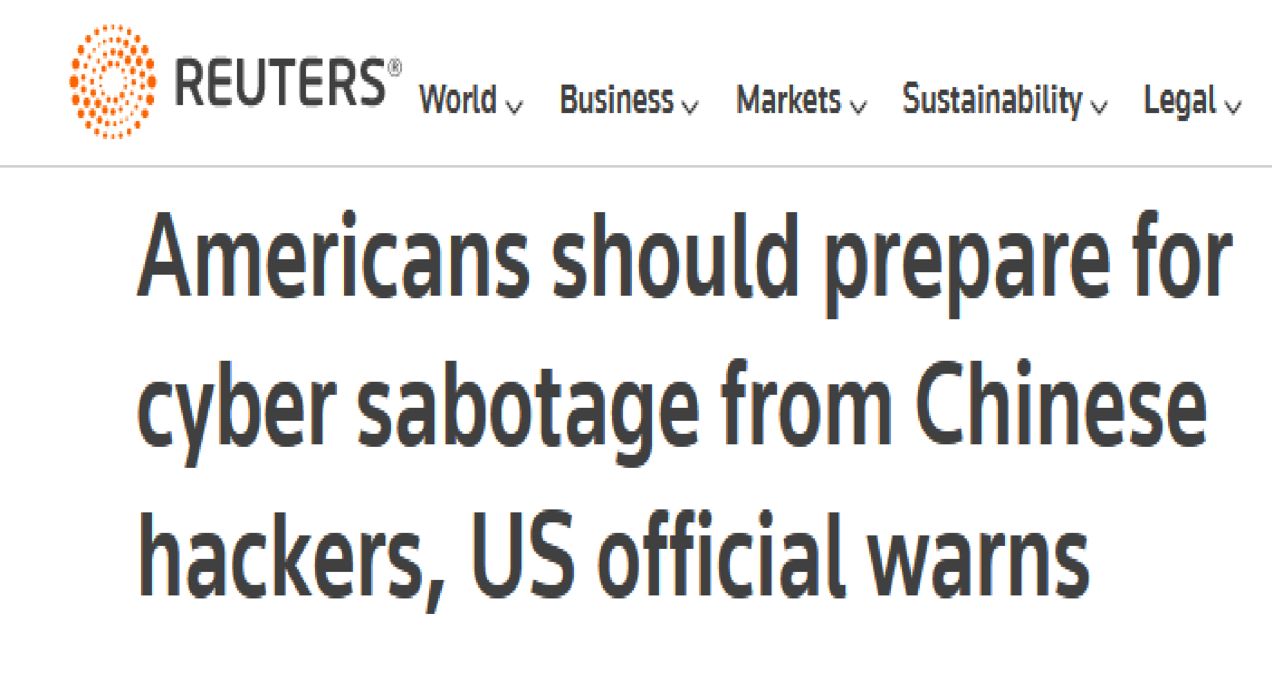
Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find



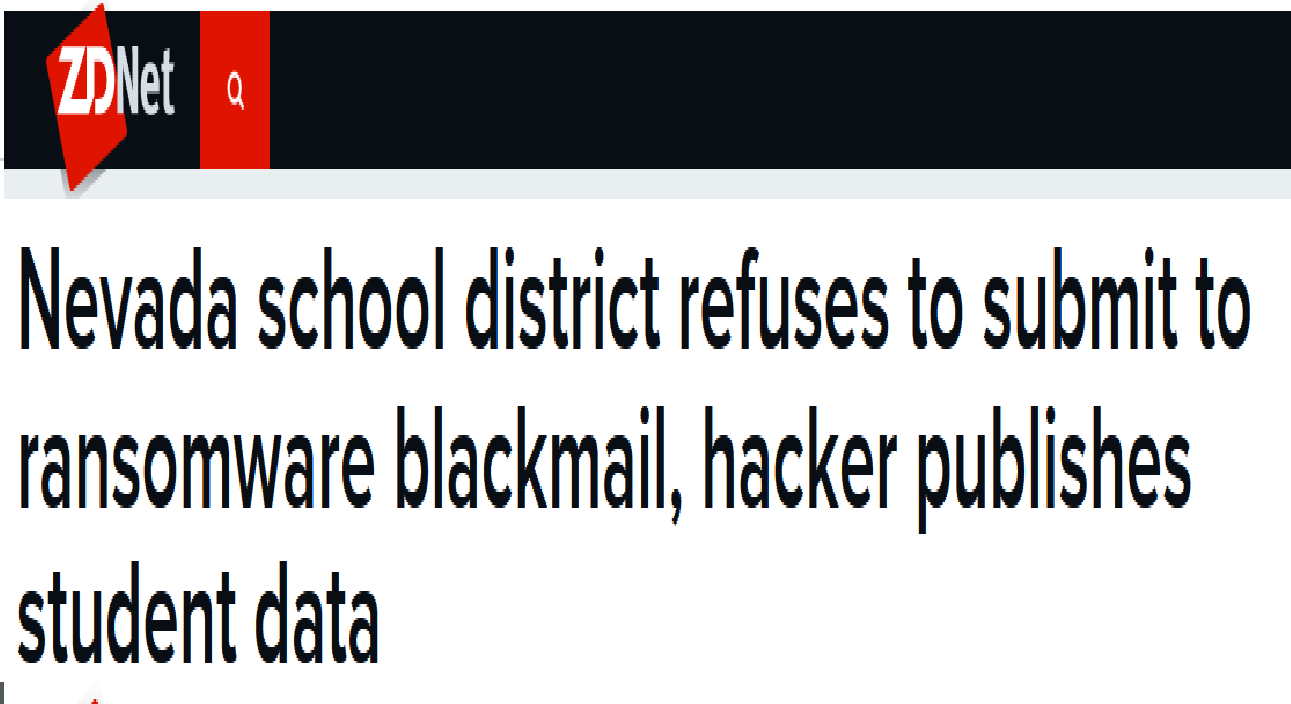
Cybercrime To Cost The World 8 Trillion Annually In 2023


PC
#AllAboutAI #UltimatePCBuildGuide Best Products Reviews How-To News

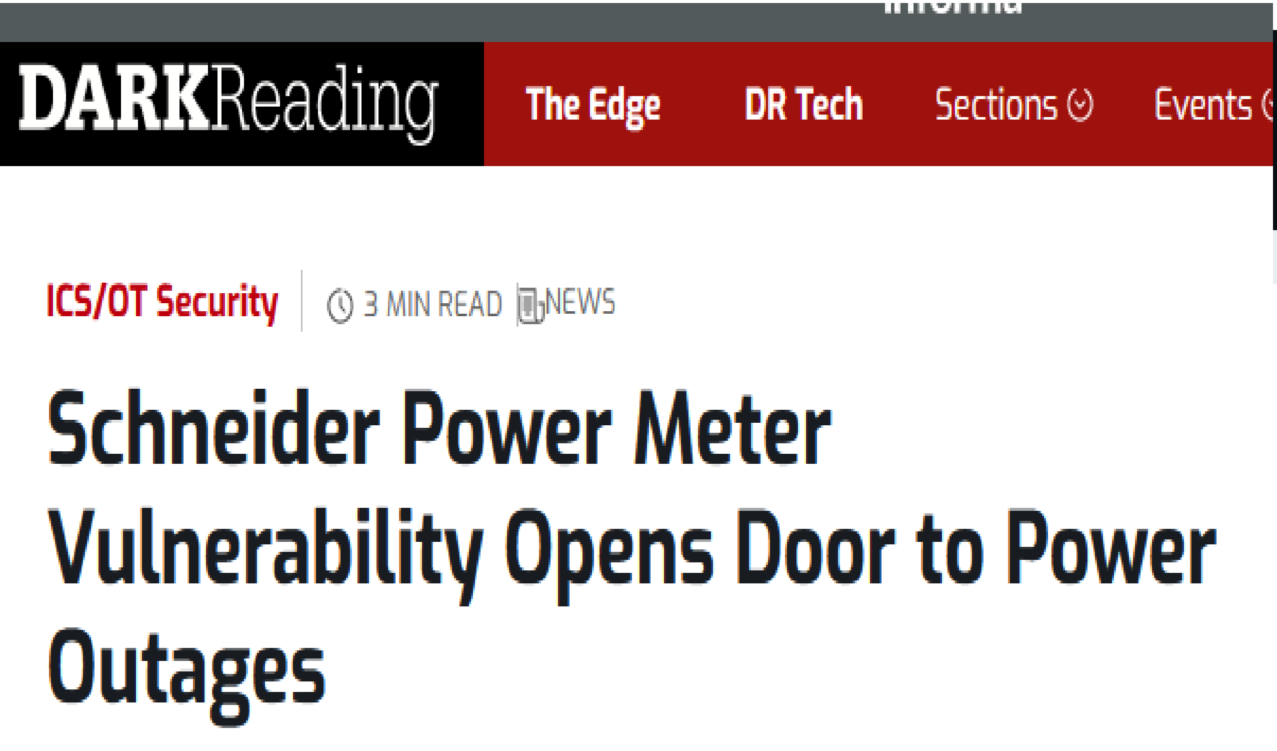
Hacker Deepfakes Employee's Voice in Phone Call to Breach IT Company



Americans should prepare for cyber sabotage from Chinese hackers, US official warns

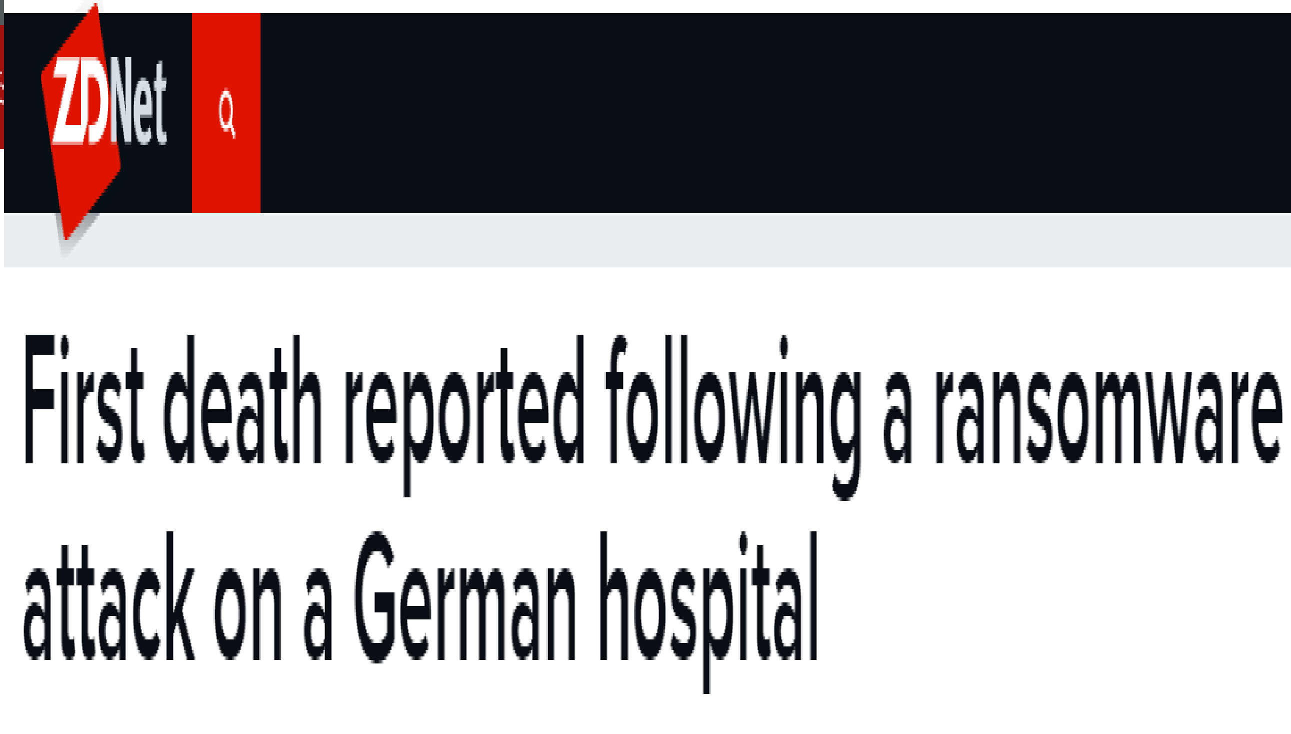


Nevada school district refuses to submit to ransomware blackmail, hacker publishes student data

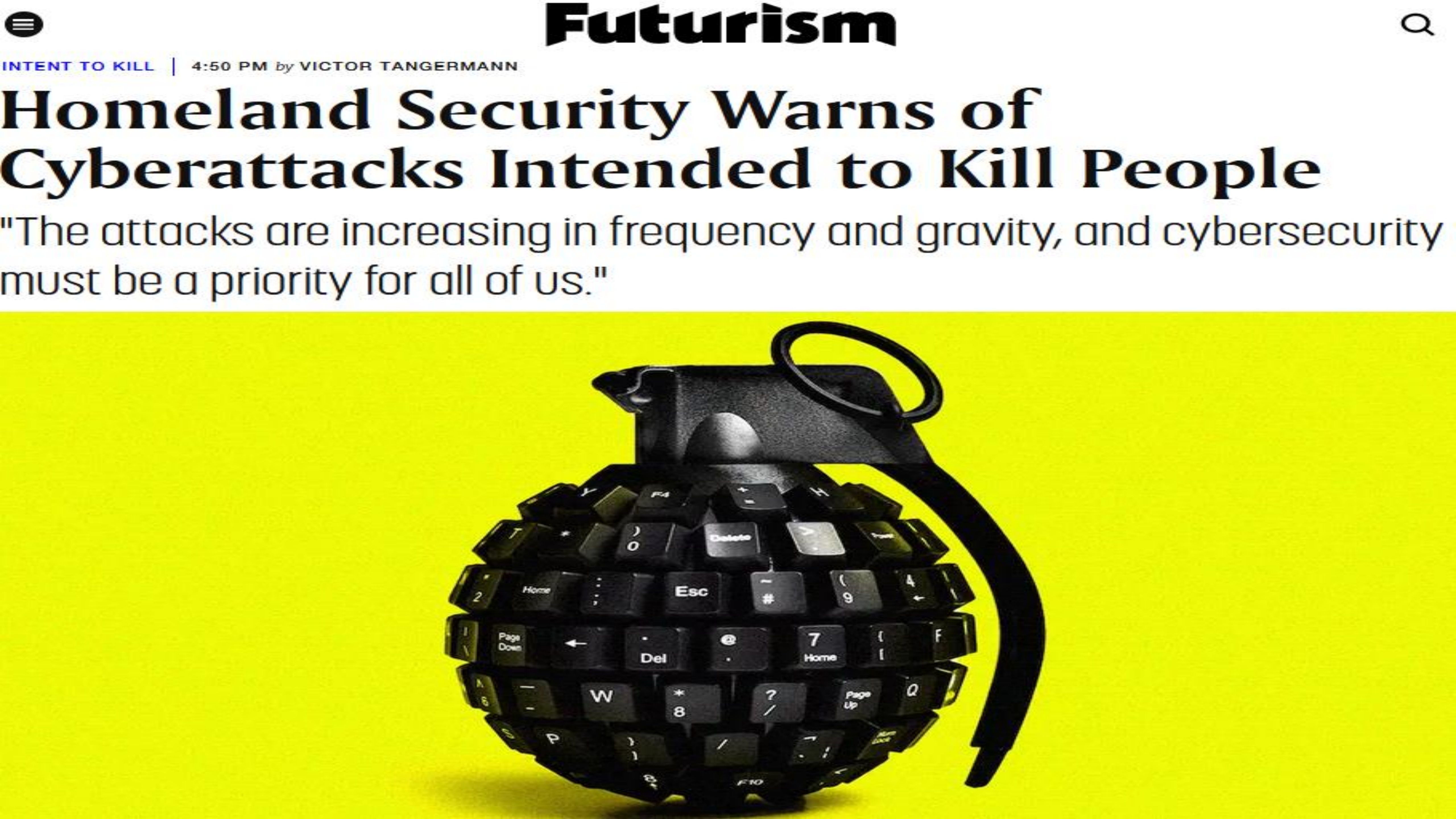


ICS/OT Security | 3 MIN READ NEWS

Schneider Power Meter Vulnerability Opens Door to Power Outages



First death reported following a ransomware attack on a German hospital



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."

Cybersecurity myths

- My organization is too small or to be a target
- My data (or the data I have access to) isn't valuable
- Attacks are always technically complex
- New software and devices are secure out-of-the-box
- Cybersecurity requires a huge financial investment
- Cyber breaches are covered by insurance
- Security is an IT issue

EVERY *minute* OF THE DAY

4K
PEOPLE READING YELP REVIEWS

174K
APPS DOWNLOADED

16.2M
TEXTS SENT

231M
EMAILS SENT

694M
SONGS STREAMED IN THE U.S.

6M
PEOPLE SHOPPING ONLINE

5.9M
GOOGLE SEARCHES

44M
PEOPLE VIEWING FACEBOOK LIVE STREAMS

12.5K
RIDE-SHARES TAKEN

20.8K
ACTIVE USERS ON LINKEDIN

2.1M
PEOPLE ACTIVE ON FACEBOOK

575K
TWEETS SENT

46K
SEARCHES ON PINTEREST

66K
PHOTOS AND VIDEOS SHARED ON INSTAGRAM

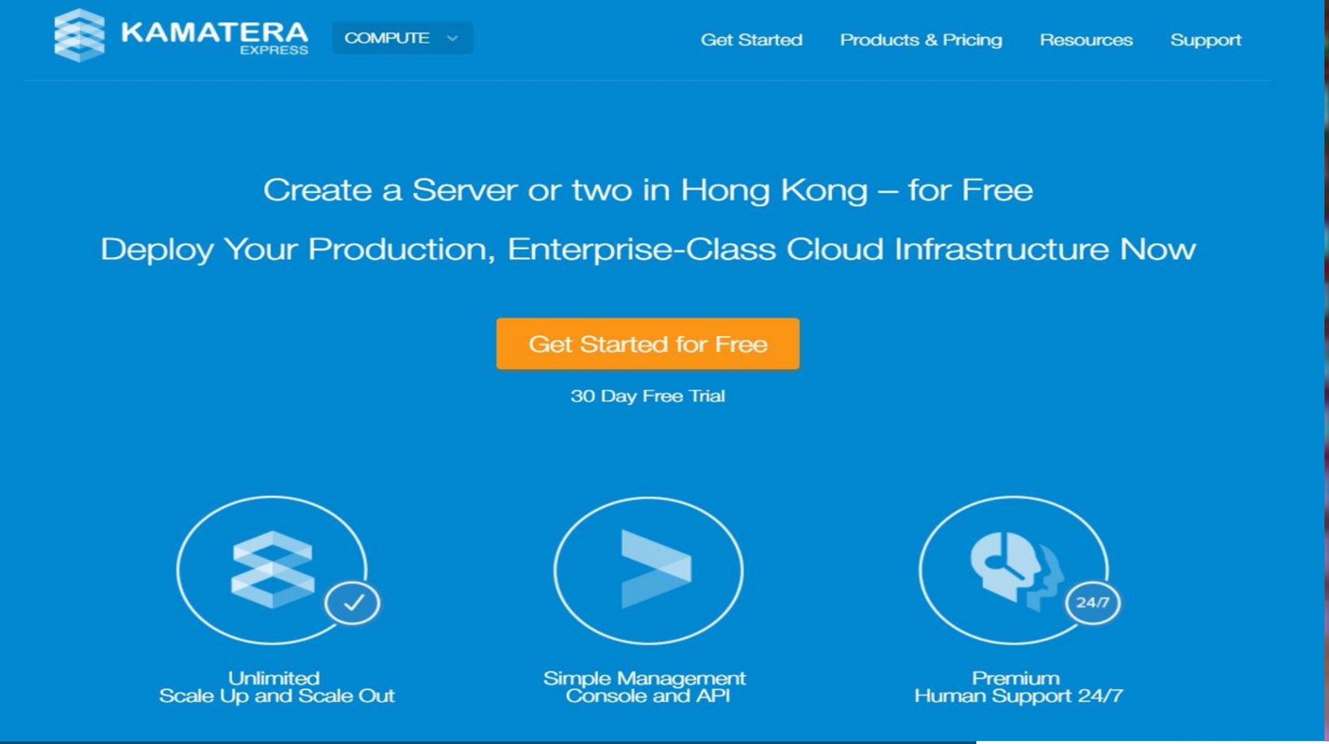
2M
SNAPCHATS SENT

167M
VIDEOS WATCHED ON TIKTOK

452K
HOURS OF CONTENT STREAMED ON NETFLIX

3.67M
YOUTUBE VIDEOS WATCHED

LOCALiQ



Create a Server or two in Hong Kong – for Free

Deploy Your Production, Enterprise-Class Cloud Infrastructure Now

30 Day Free Trial

Unlimited
Scale Up and Scale Out

Simple Management
Console and API

Premium
Human Support 24/7

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

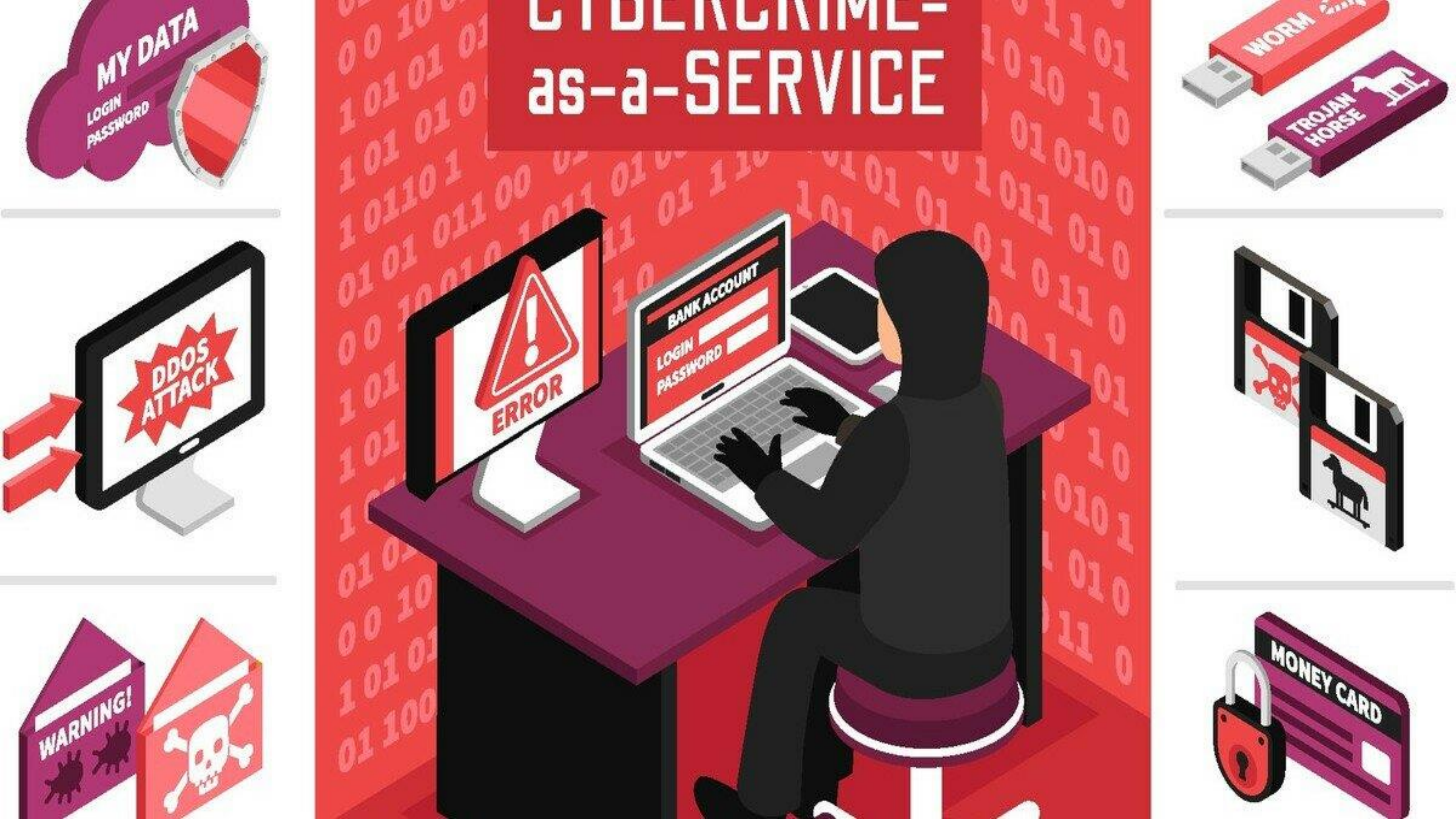
- Economic gain
- Significant technical resources and capabilities
- Established syndicates
- Adware, crimeware, IP theft

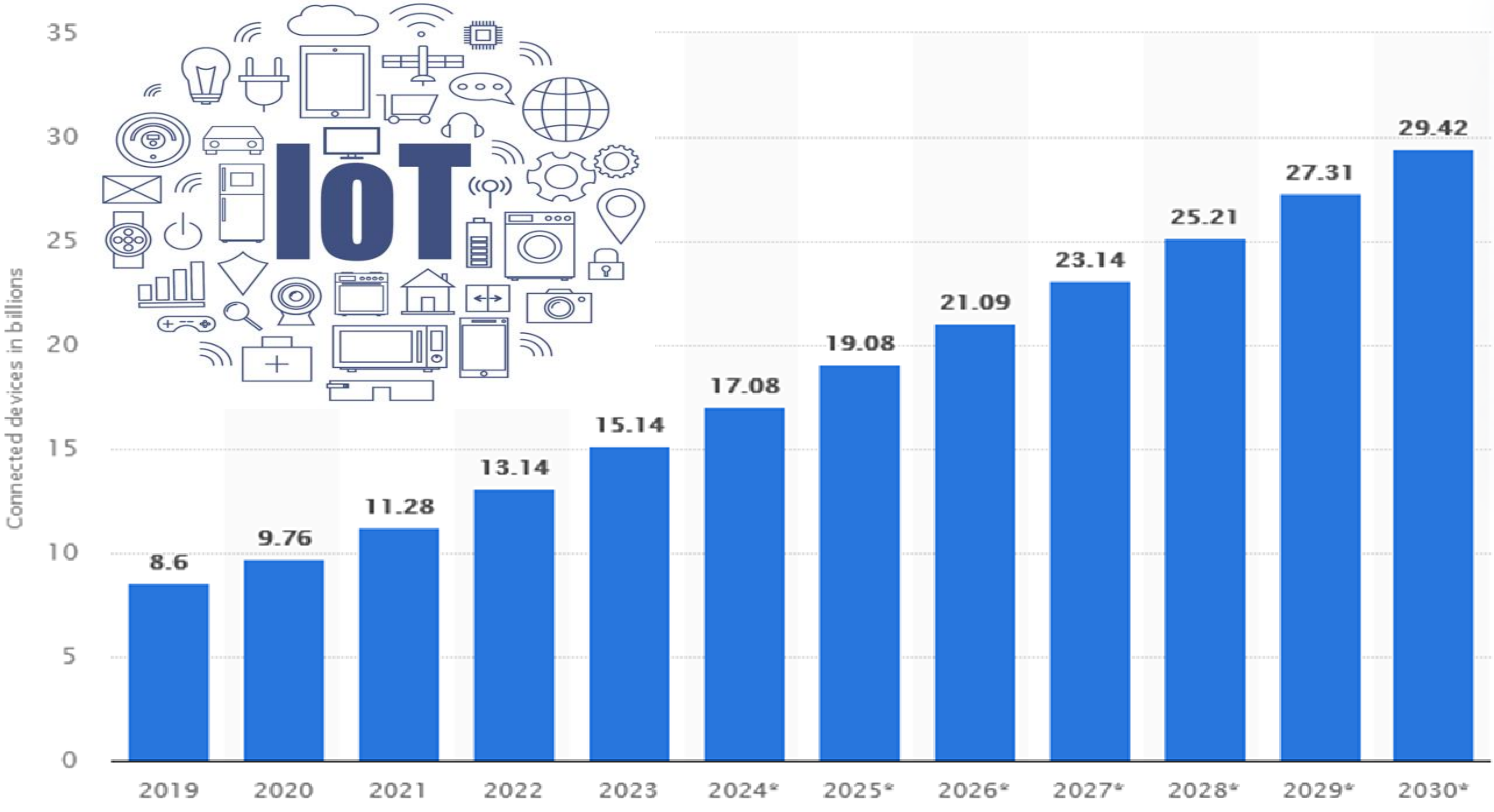
State Sponsored

- 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.


CYBERCRIME-
as-a-SERVICE
MY DATA
LOGIN
PASSWORD
DDOS ATTACK
WARNING!
ERROR
BANK ACCOUNT
LOGIN
PASSWORD
WORM
TROJAN HORSE
MONEY CARD



© Statista 2024

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.

Bank Account Info

⊞ 🤖 📱
- Downloaded bank statements

Recent Files

⊞
- List kept by operating system

⊞ 🤖 📱
- Various applications keep their own recent file lists

Contacts

- ⊞ Windows Contacts
- Address Book
- 🤖 📱 Contact manager

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

Text Messages

- 📱 Text log stored on phone

Phone Calls

- 📱 Call log stored on phone

Name and Address

- ⊞ Web browser autofill
- ⊞ Windows Contacts
- Address Book
- 🤖 📱 Contact manager

Recently Visited Sites

⊞ 🤖 📱
- Browser's cache
- Browser's history
- Cookies

Current Location

🤖 📱
- Readable off your GPS

Recent Locations

🤖 📱
- Photos
- Navigation apps

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	With bank info	Fullz info*
$5	$15	$30

Drivers license

$20

Loyalty accounts

$20

General non-financial institution logins

$1

Diplomas

$100-$400

Passports (US)

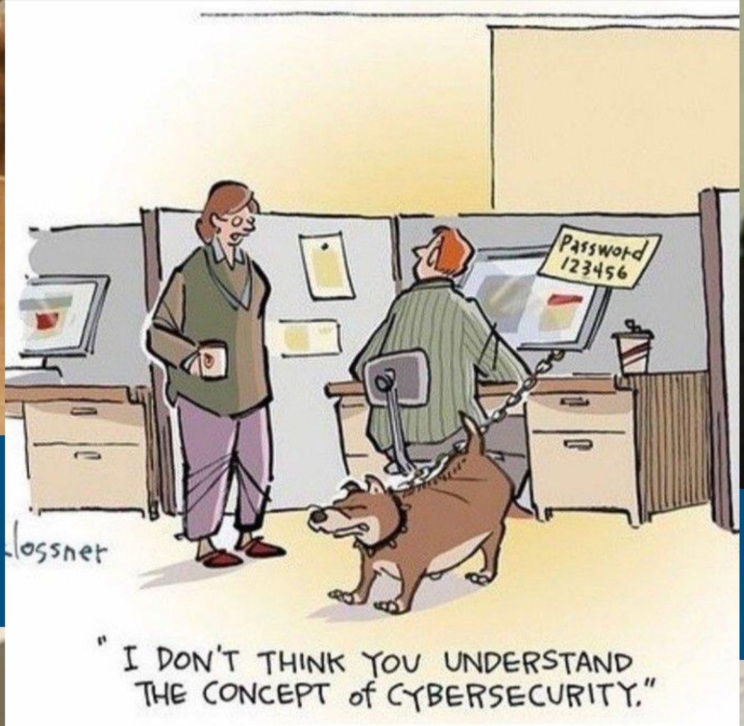
$1000-$2000

Subscription services

$1-$10

Medical records

$1-$1000**


Password
123456
Glossner
"I DON'T THINK YOU UNDERSTAND THE CONCEPT of CYBERSECURITY."

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

"Only amateurs attack machines; professionals target people." – Bruce Schneier

Guiding principals of security

- Nothing is foolproof
- Focus on risk
- Take a layered approach – Defense In Depth
- 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

TOP 15 CYBER THREATS

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

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

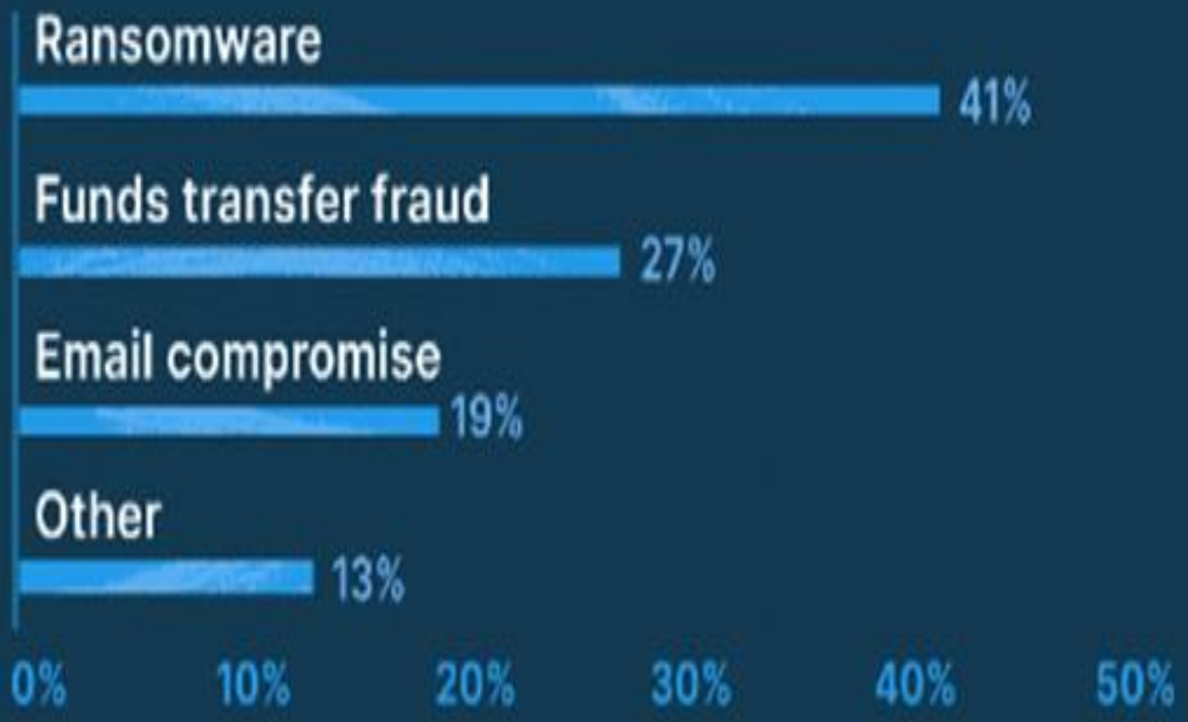
12 Information leakage

13 Ransomware

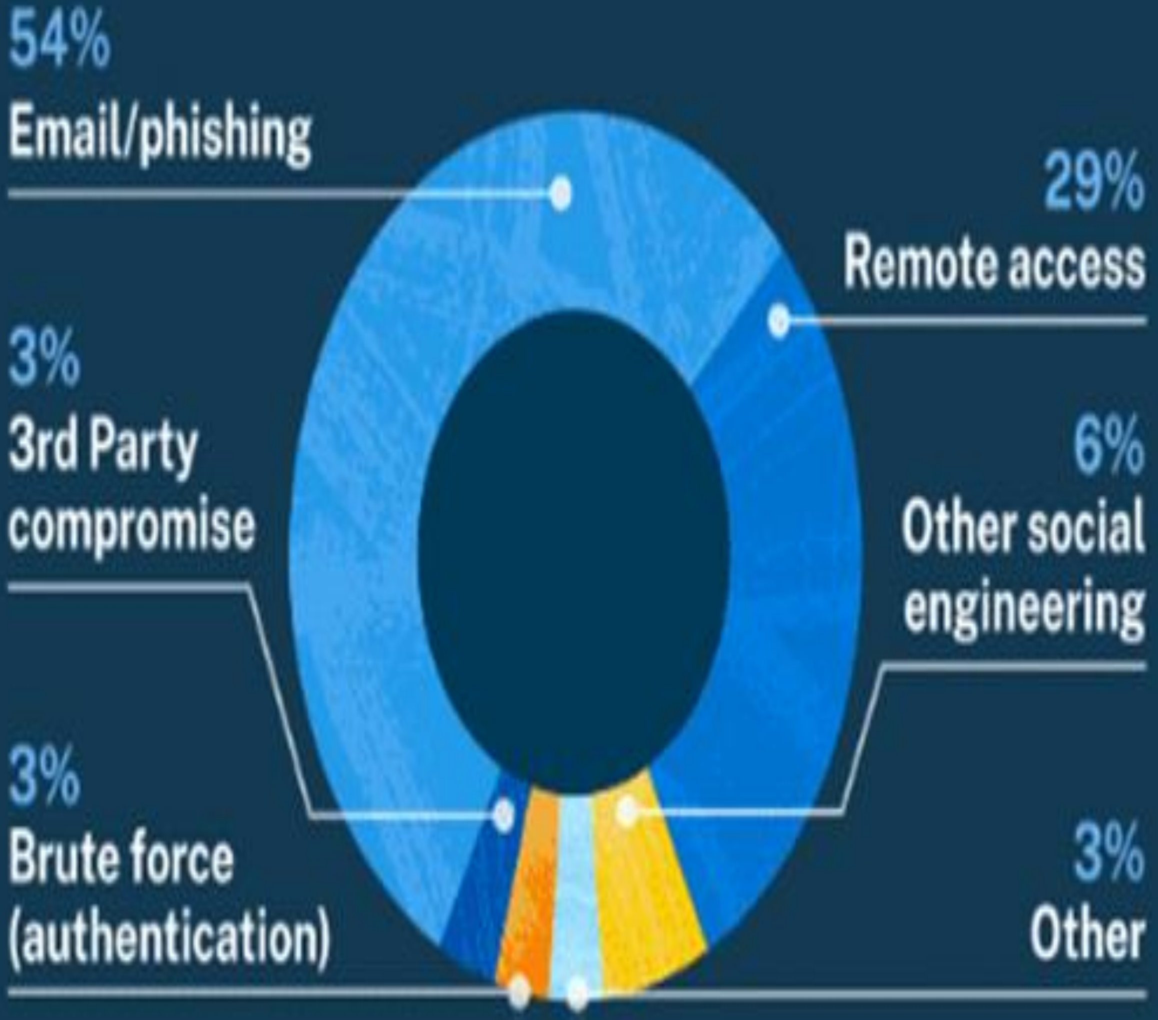
14 Cyberespionage

15 Cryptojacking

Most common cyber incidents (% of reported claims)



Percentage of claims by attack technique

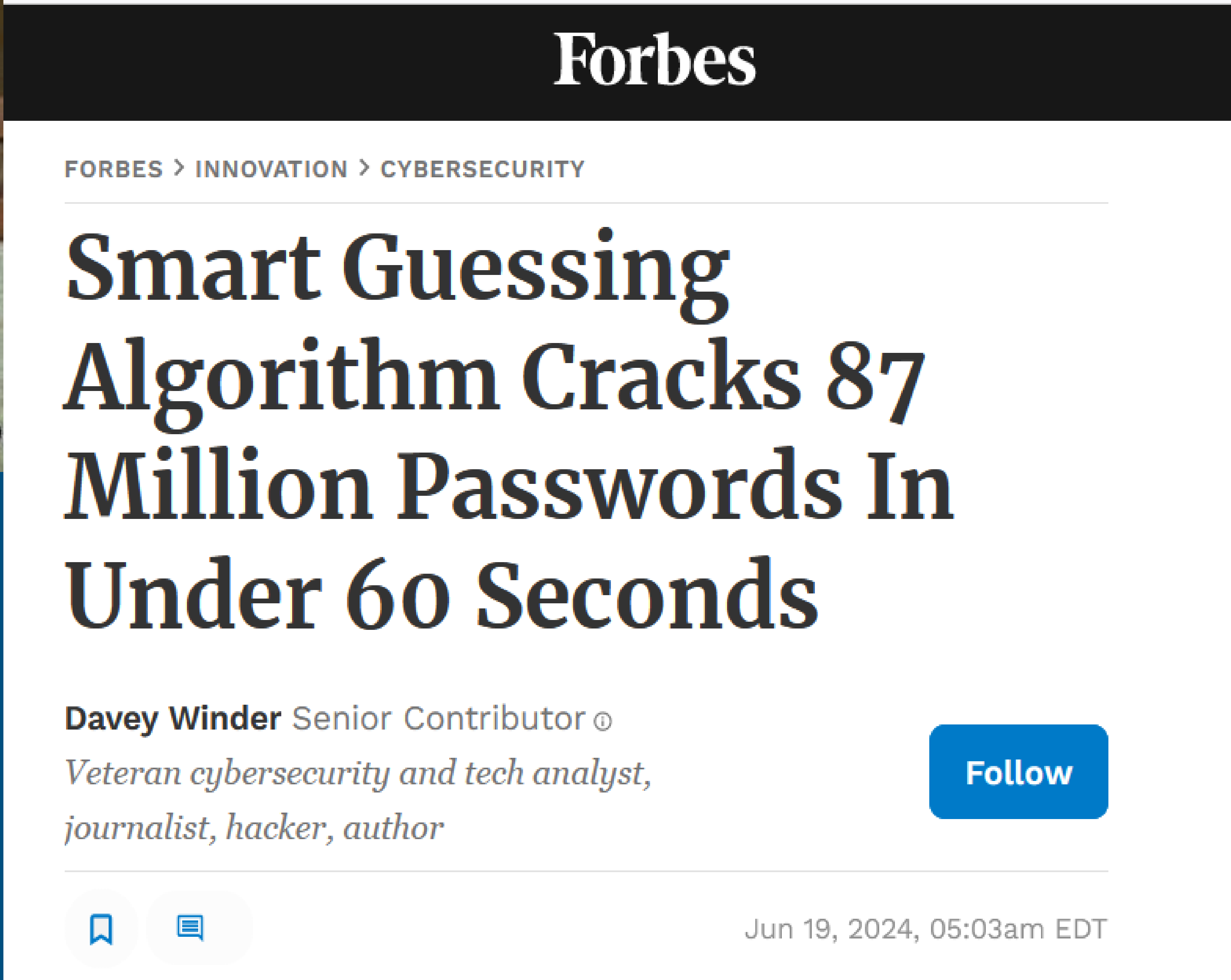


I changed all my passwords to "incorrect".

So whenever I forget, it will tell me "Your password is incorrect."

Sorry password must contain a special character

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



Forbes

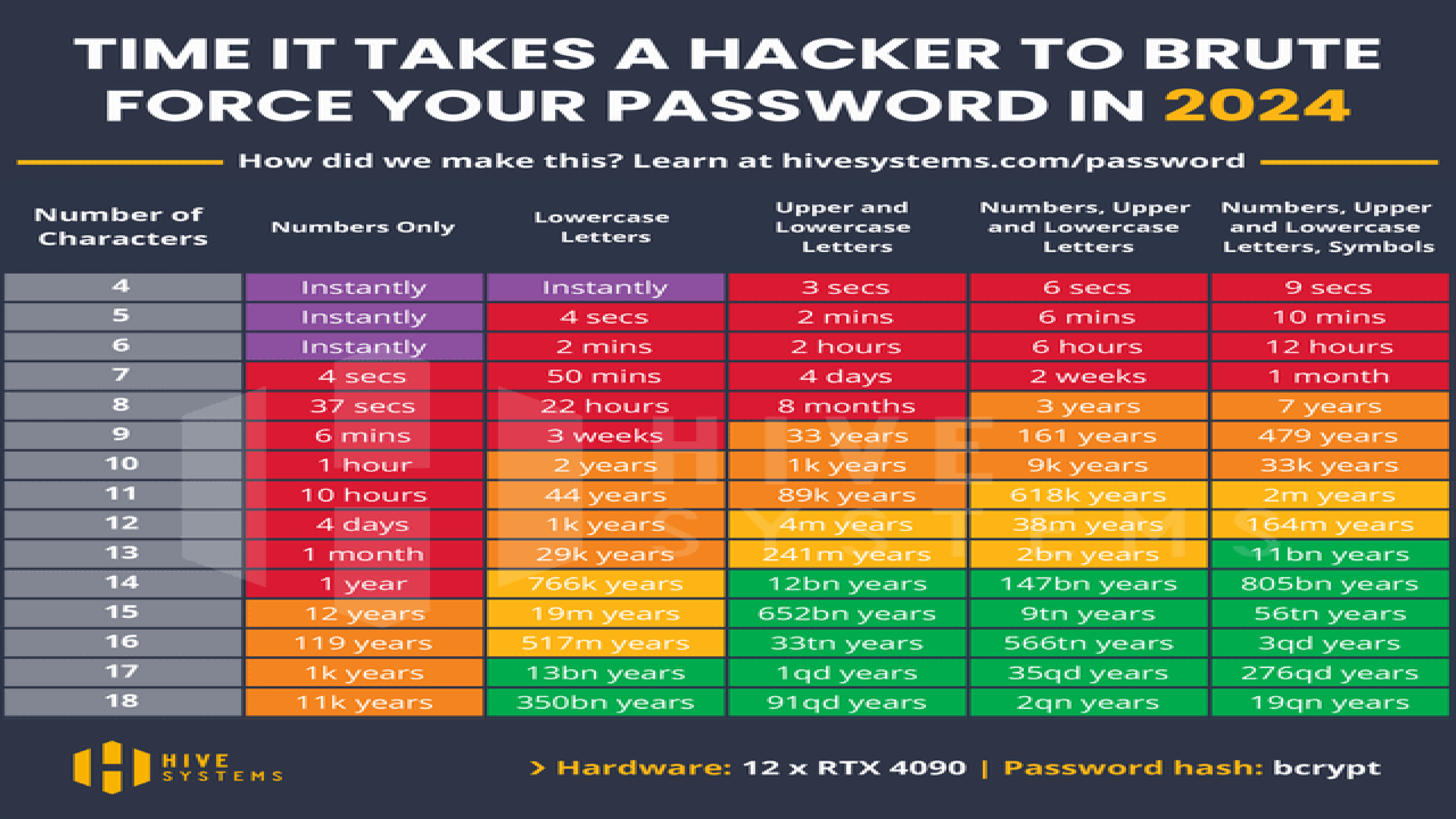
FORBES › INNOVATION › CYBERSECURITY

Smart Guessing Algorithm Cracks 87 Million Passwords In Under 60 Seconds

Davey Winder Senior Contributor

Veteran cybersecurity and tech analyst, journalist, hacker, author

Jun 19, 2024, 05:03am EDT

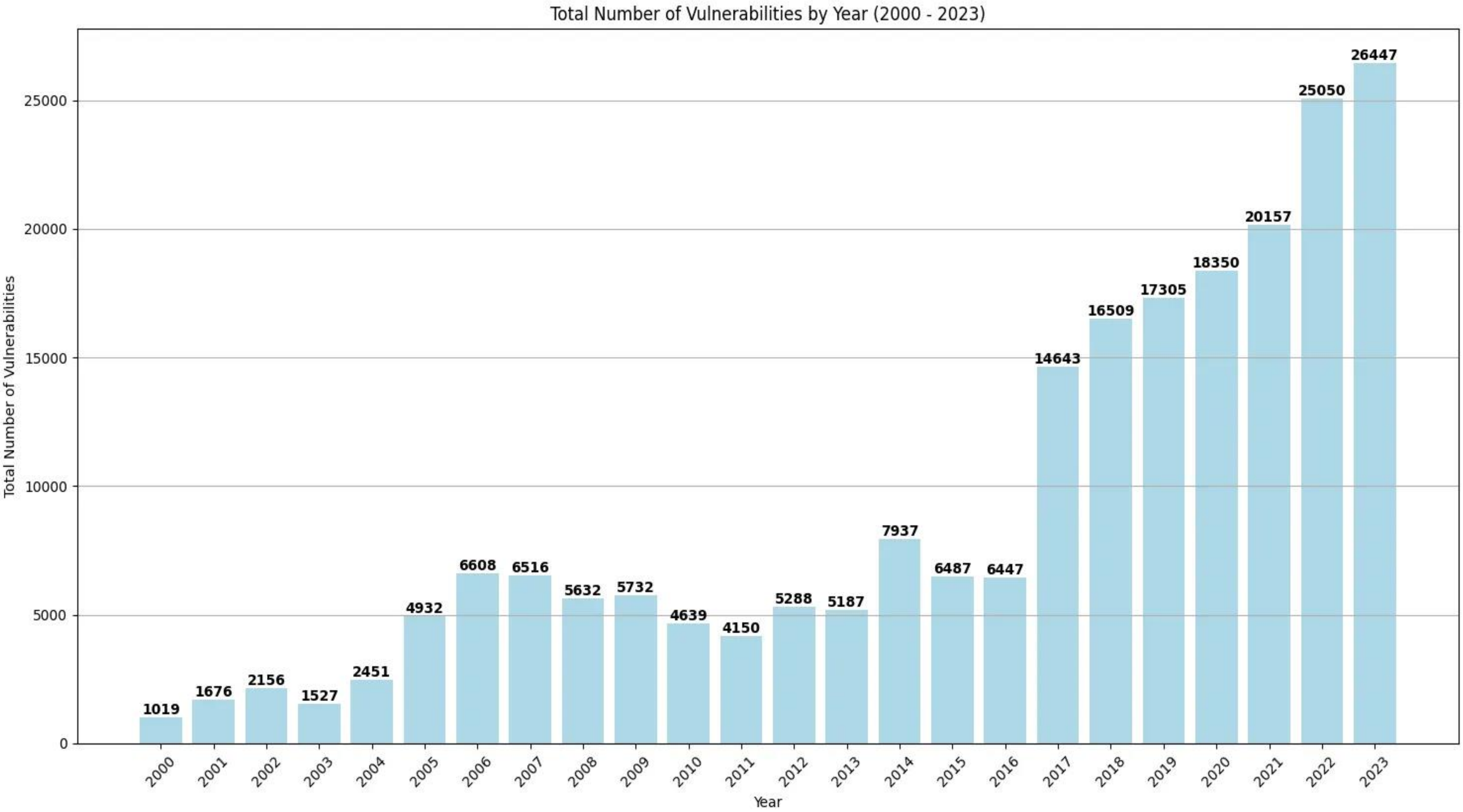


TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

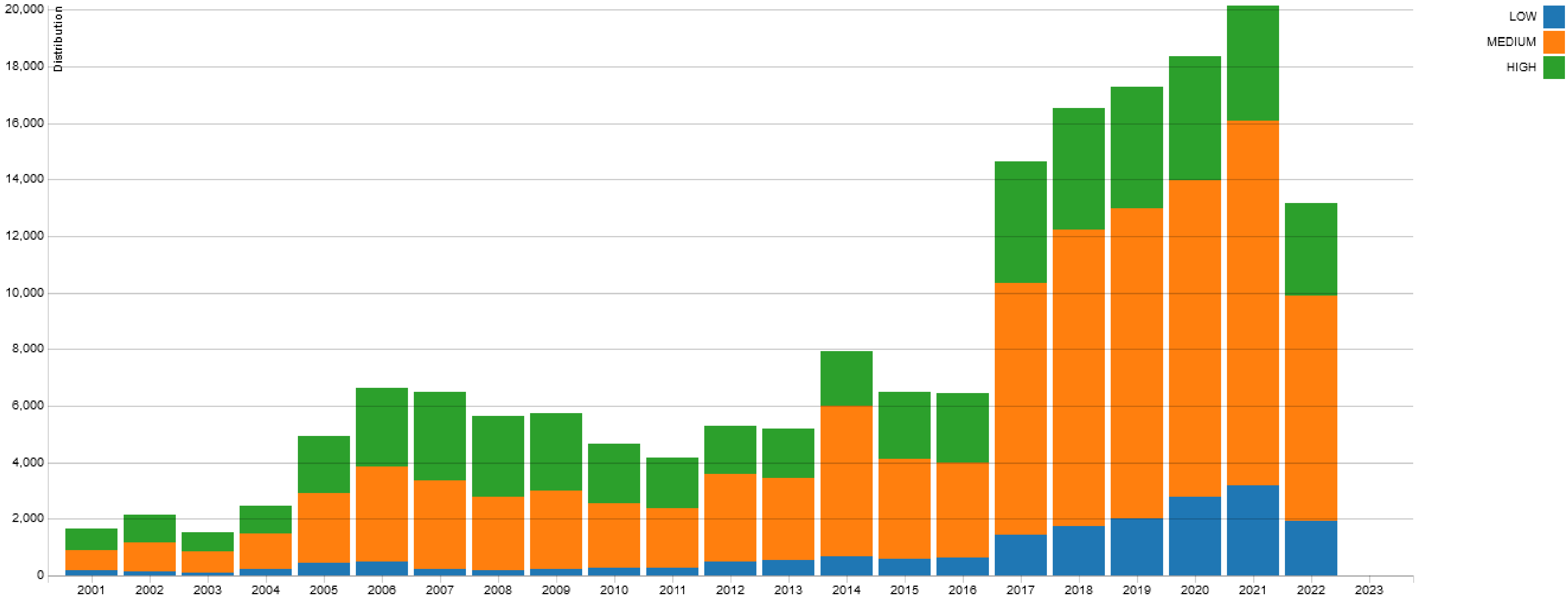
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

> Hardware: 12 x RTX 4090 | Password hash: bcrypt


Total Number of Vulnerabilities by Year (2000 - 2023)
Total Number of Vulnerabilities
Year
0
5000
10000
15000
20000
25000
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
1019
1676
2156
1527
2451
4932
6608
6516
5632
5732
4639
4150
5288
5187
7937
6487
6447
14643
16509
17305
18350
20157
25050
26447

CVSS Severity Distribution Over Time

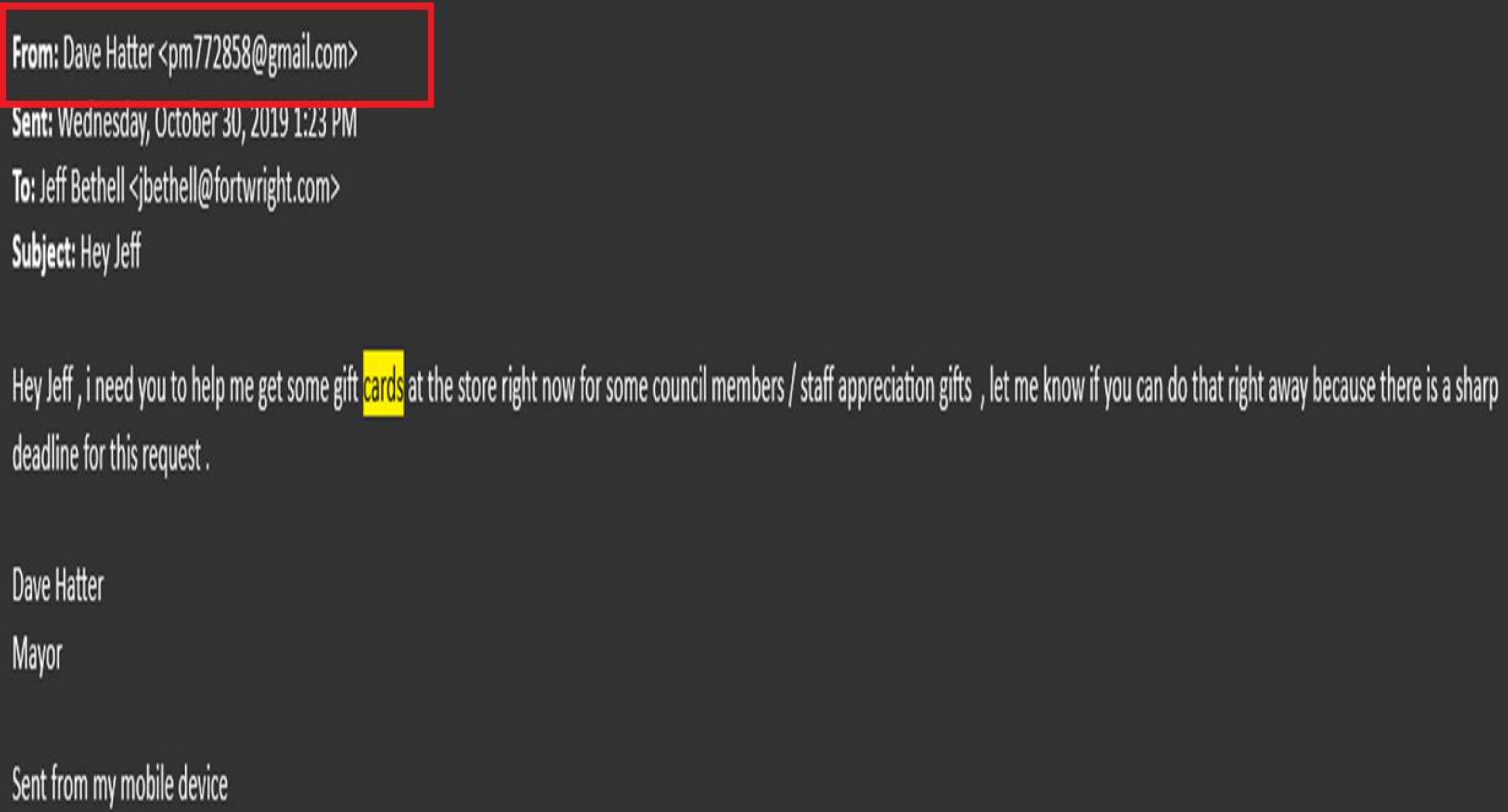
This visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score. For more information on how this data was constructed please see the NVD CVSS page .



Spoofing

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

"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



From: Dave Hatter <pm772858@gmail.com>

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

To: Jeff Bethell <jbethell@fortwright.com>

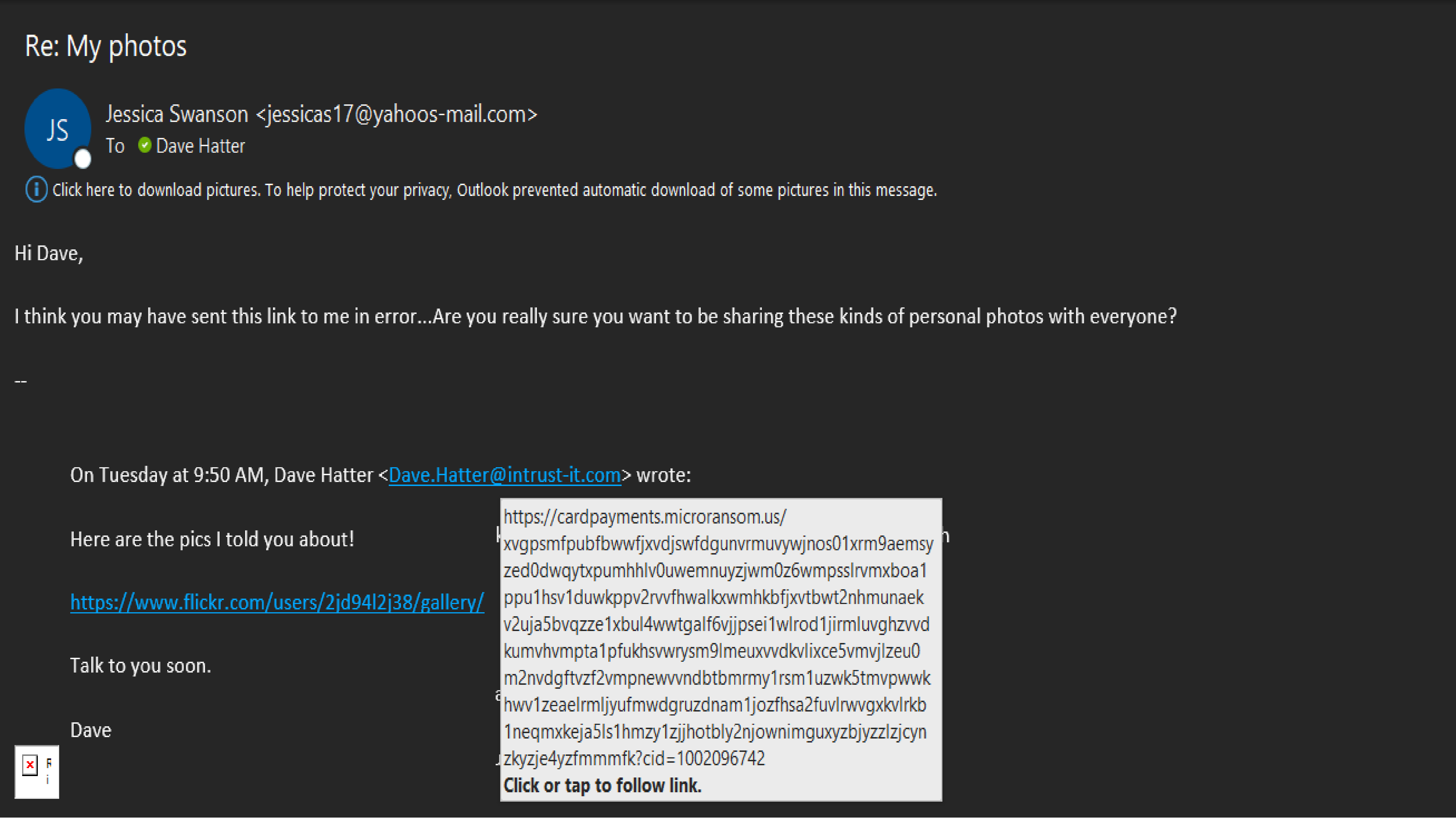
Subject: Hey Jeff

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



Re: My photos

JS

Jessica Swanson <jessicas17@yahoos-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,

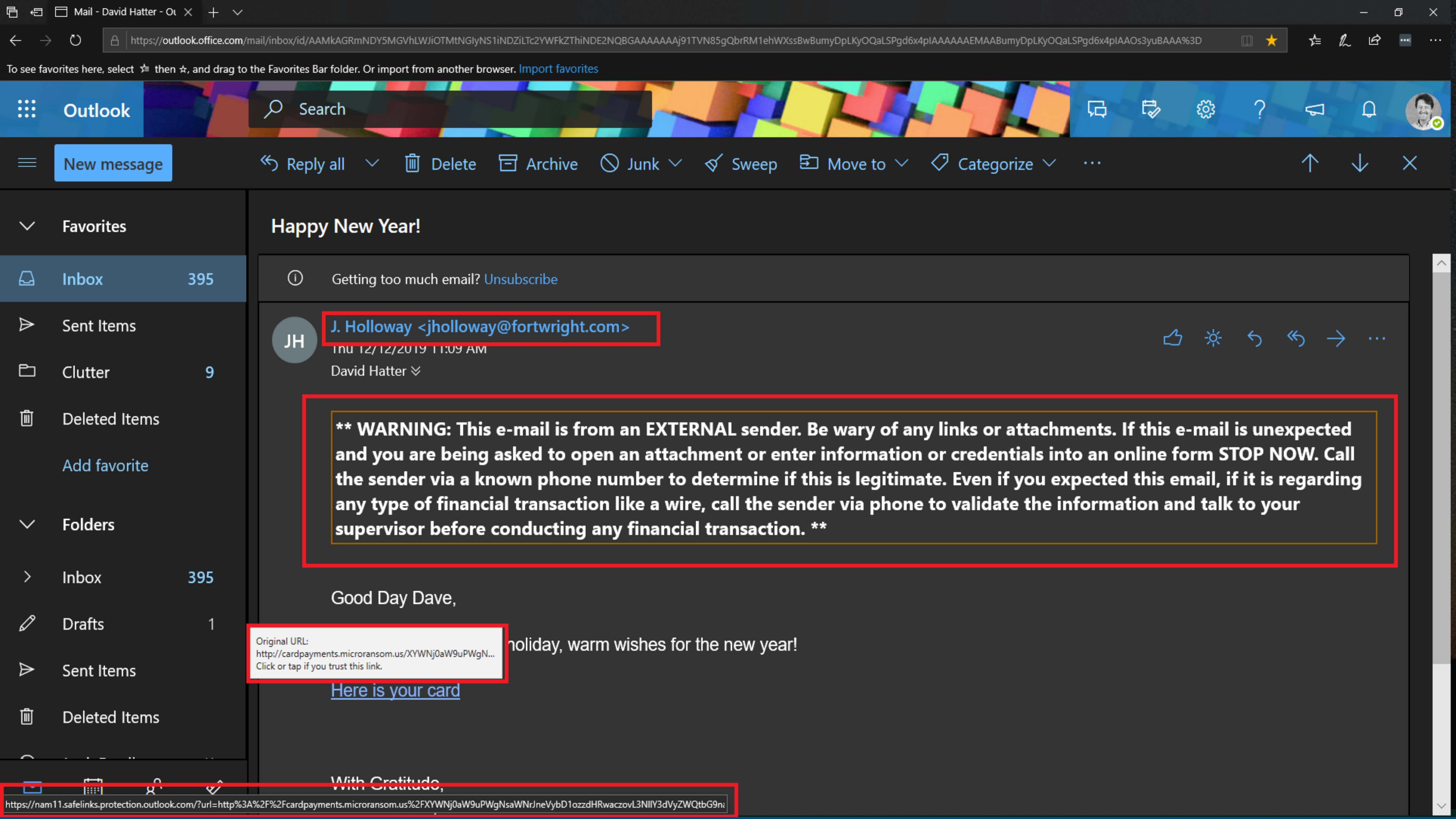
I think you may have sent this link to me in error...Are you really sure you want to be sharing these kinds of personal photos with everyone?

--

> 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/
xvgpsmfpubfbwwfjxvdjswfdgunvrmuvywjnos01xrm9aemsy
zed0dwqytxpumhhlv0uwemnuyzjwm0z6wmpsslrvmxboa1
ppu1hsv1duwkppv2rvvfhwalkxwmhkbfjxvtbwt2nhmunaek
v2uja5bvqzze1xbul4wwtgalf6vjjpsei1wlrod1jirmluvghzvvd
kumvhvmpta1pfukhsvwrysm9lmeuxvvdkvlixce5vmvjlzeu0
m2nvdgftvzf2vmpnewvvndbtbmrmy1rsm1uzwk5tmvpwwk
hwv1zeaelrmljyufmwdgruzdnam1jozfhsa2fuvlrwvgxkvlrkb
1neqmxkeja5ls1hmzy1zjjhotbly2njownimguxyzbjyzzlzjcyn
zkyzje4yzfmmmfk?cid=1002096742
```

Click or tap to follow link.



https://outlook.office.com/mail/inbox/id/AAMkAGRmNDY5MGVhLWJiOTMtNGlyNS1iNDZiLTc2YWFkZThiNDE2NQBGAAAAAAAj91TVN85gQbrRM1ehWXssBwBumyDpLKyOQaLSPgd6x4pIAAAAAAEMAABumyDpLKyOQaLSPgd6x4pIAAOs3yuBAAA%3D

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,

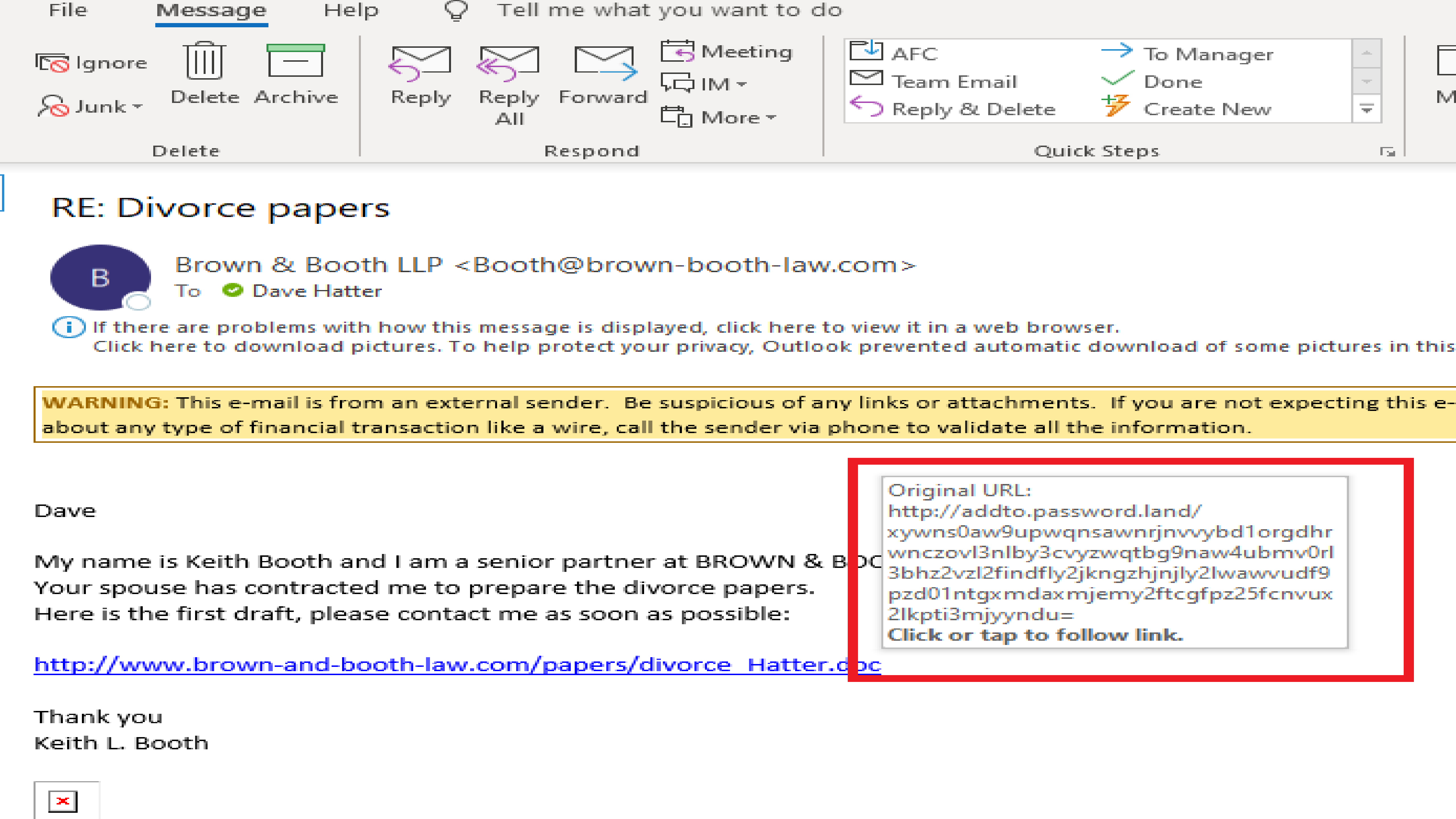
Original URL:
http://cardpayments.microransom.us/XYWNj0aW9uPWgN...
Click or tap if you trust this link.

holiday, warm wishes for the new year!

Here is your card

With Gratitude,

https://nam11.safelinks.protection.outlook.com/?url=http%3A%2F%2Fcardpayments.microransom.us%2FXYWNj0aW9uPWgNsaWNrJneVybD1ozzdHRwaczovL3NlIY3dVyZWQtbG9na



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.

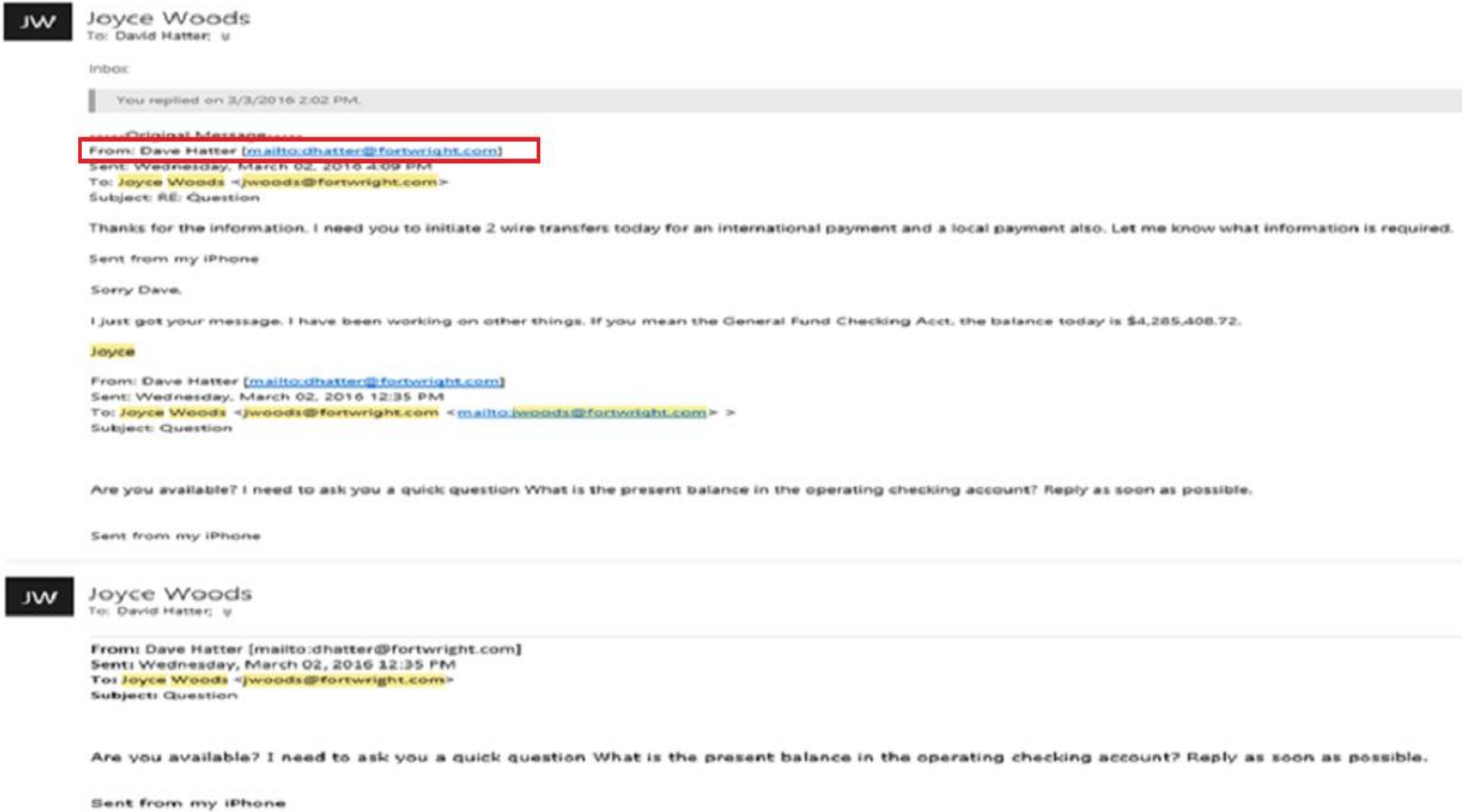
Dave

My name is Keith Booth and I am a senior partner at BROWN & BOC
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

Original URL:
http://addto.password.land/xywns0aw9upwqnsawnrjnvvybd1orgdhrwnczovl3nlby3cvyzwqtbg9naw4ubmv0rl3bhz2vzl2findfly2jkngzhjnjly2lwawvudf9pzd01ntgxmdaxmjemy2ftcgfpz25fcnvux2lkpti3mjyyndu=
Click or tap to follow link.

Thank you
Keith L. Booth



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

Forbes ADVISOR

5 EXAMPLES OF SMISHING ATTACKS

Bank Fraud Alert

A text from your bank saying there's suspicious activity on your account.

Tech Support

A text warning that your computer has a virus.

Gift Card Winnings

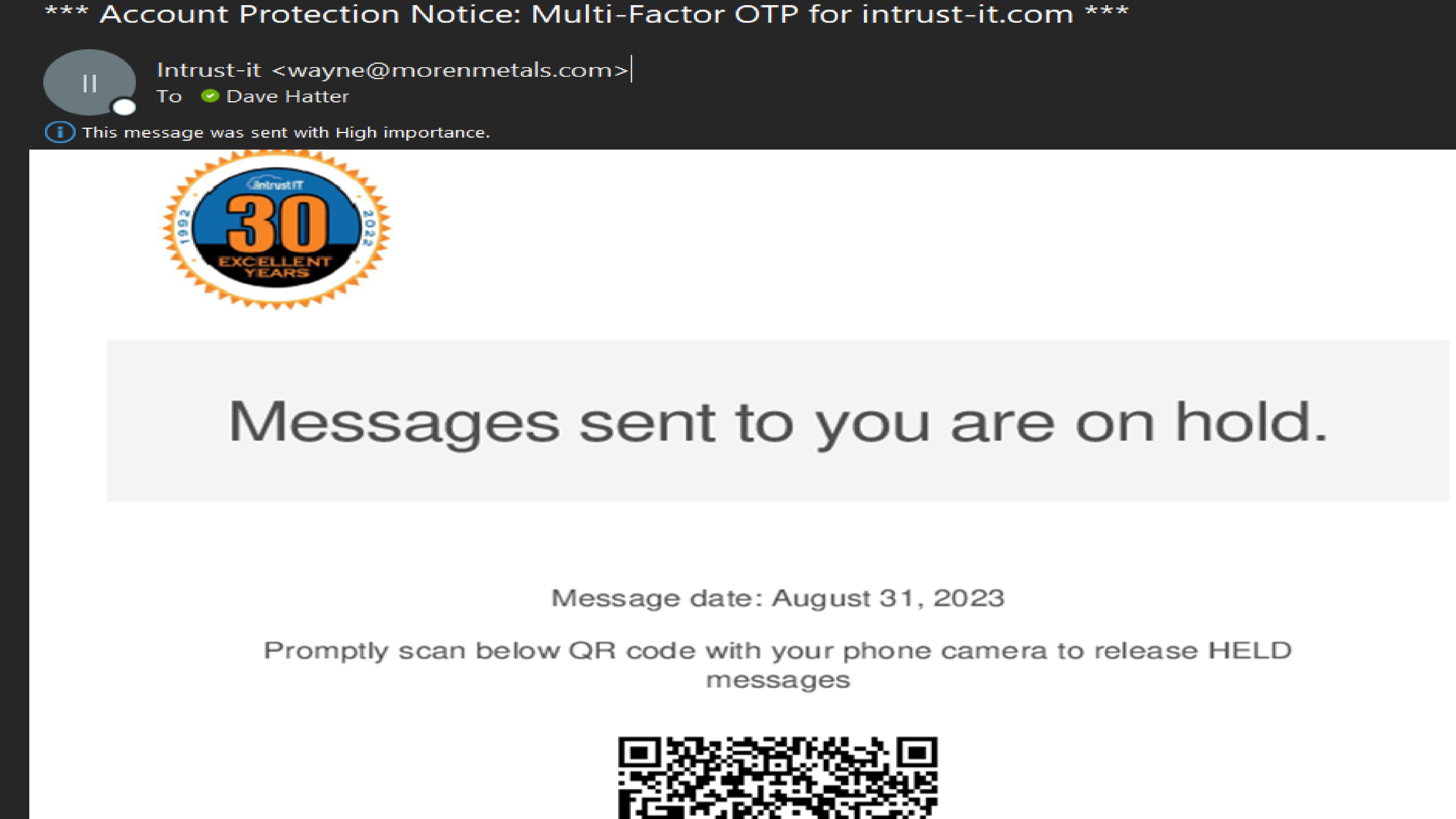
A message saying you won a gift card and need to click a link to claim it.

Missed Delivery Notification

A message saying you missed a package delivery and asks you to click a link to reschedule.

Account Verification

A message asking you to verify your account details by following a link.



*** Account Protection Notice: Multi-Factor OTP for intrust-it.com ***

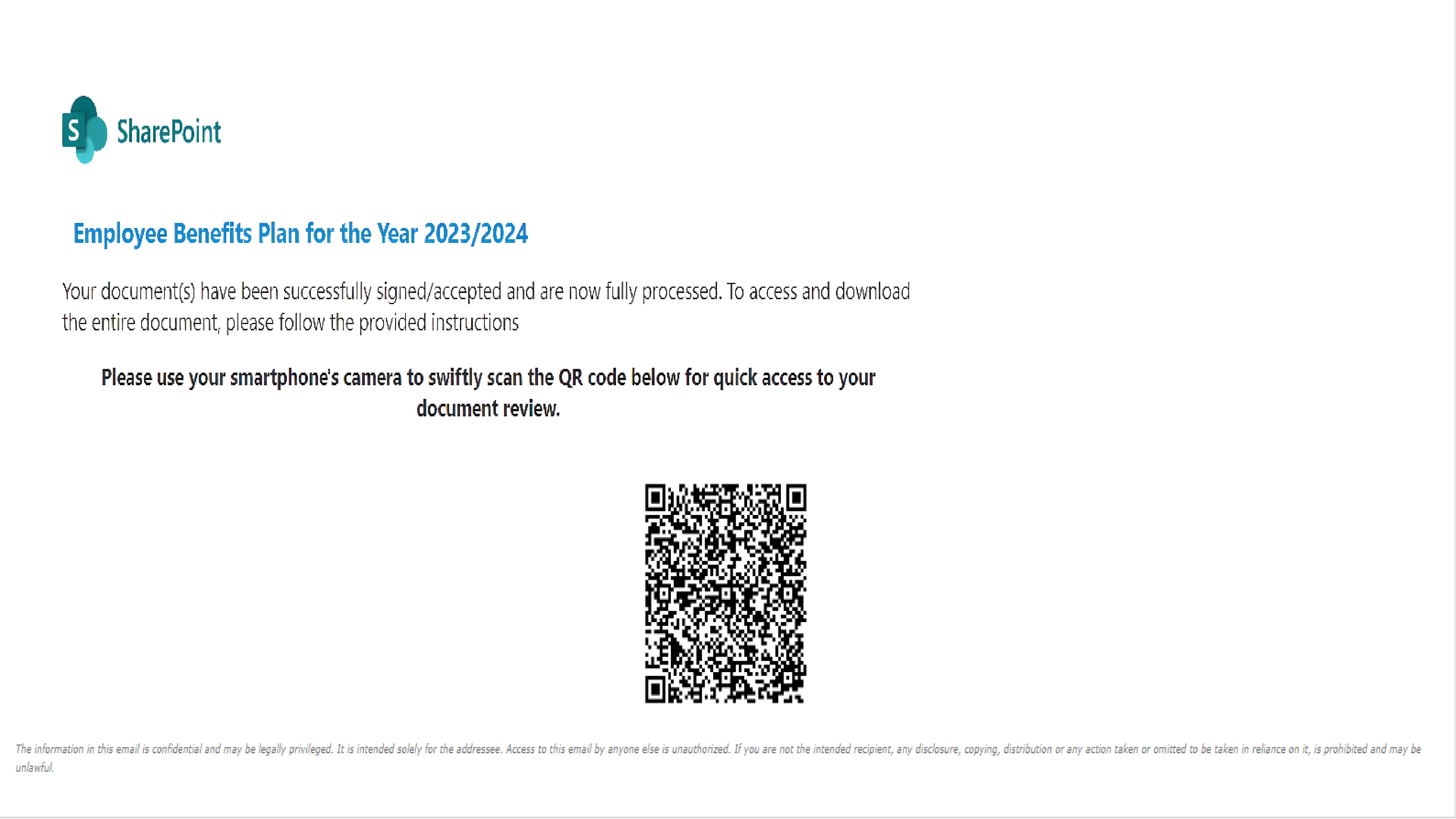
Intrust-it <wayne@morenmetals.com>
To Dave Hatter

This message was sent with High importance.

Messages sent to you are on hold.

Message date: August 31, 2023

Promptly scan below QR code with your phone camera to release HELD messages



SharePoint

Employee Benefits Plan for the Year 2023/2024

Your document(s) have been successfully signed/accepted and are now fully processed. To access and download the entire document, please follow the provided instructions

Please use your smartphone's camera to swiftly scan the QR code below for quick access to your document review.

The information in this email is confidential and may be legally privileged. It is intended solely for the addressee. Access to this email by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful.

Listen how AI can clone your voice, use it in phishing scams

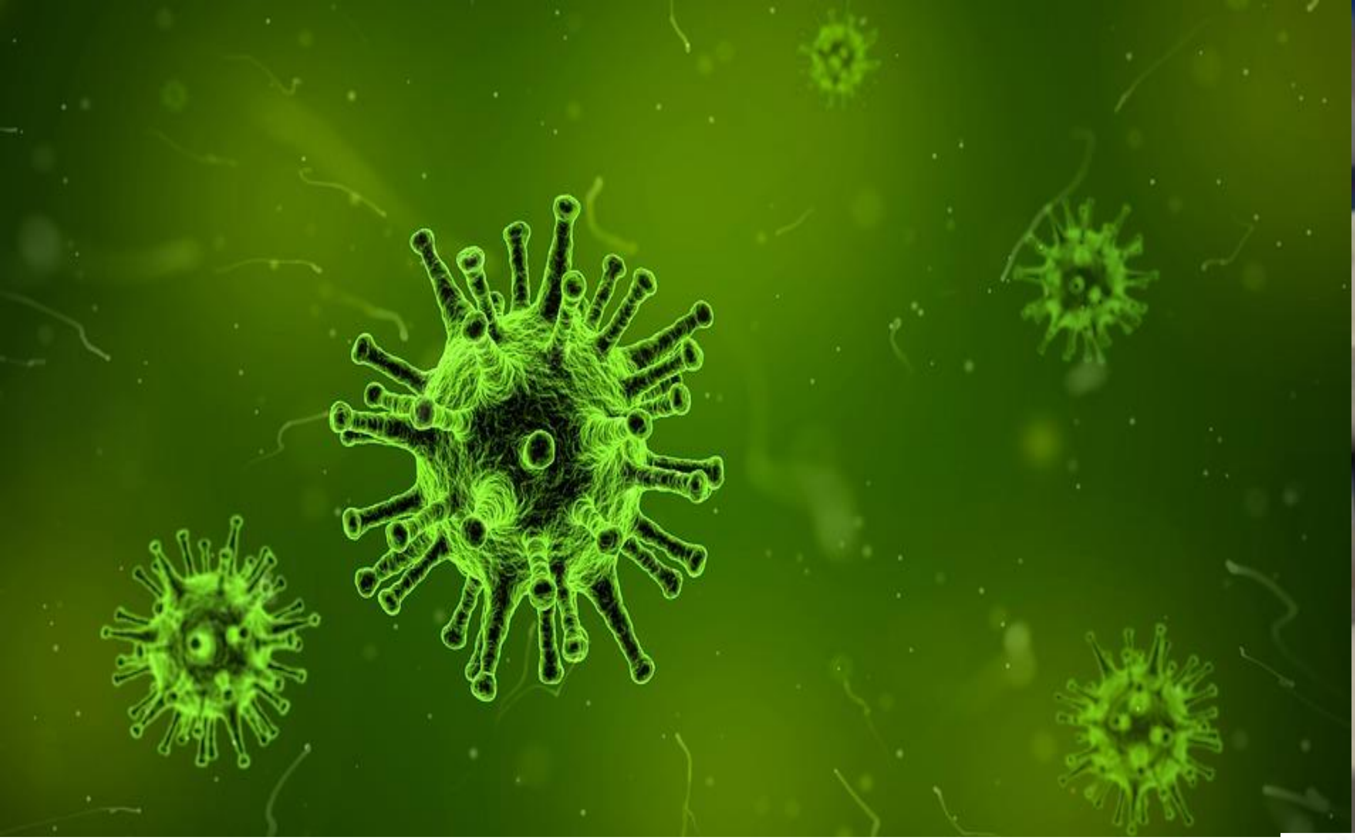
Reporter's words recorded, then turned into the "Grandparent scam"

Scammers can now use AI to clone your voice, then make scam phishing phone calls to relatives. We find out how easily it can be done, and what it sounds like.

DON'T WA$TE YOUR MONEY

Don't Waste Your Money

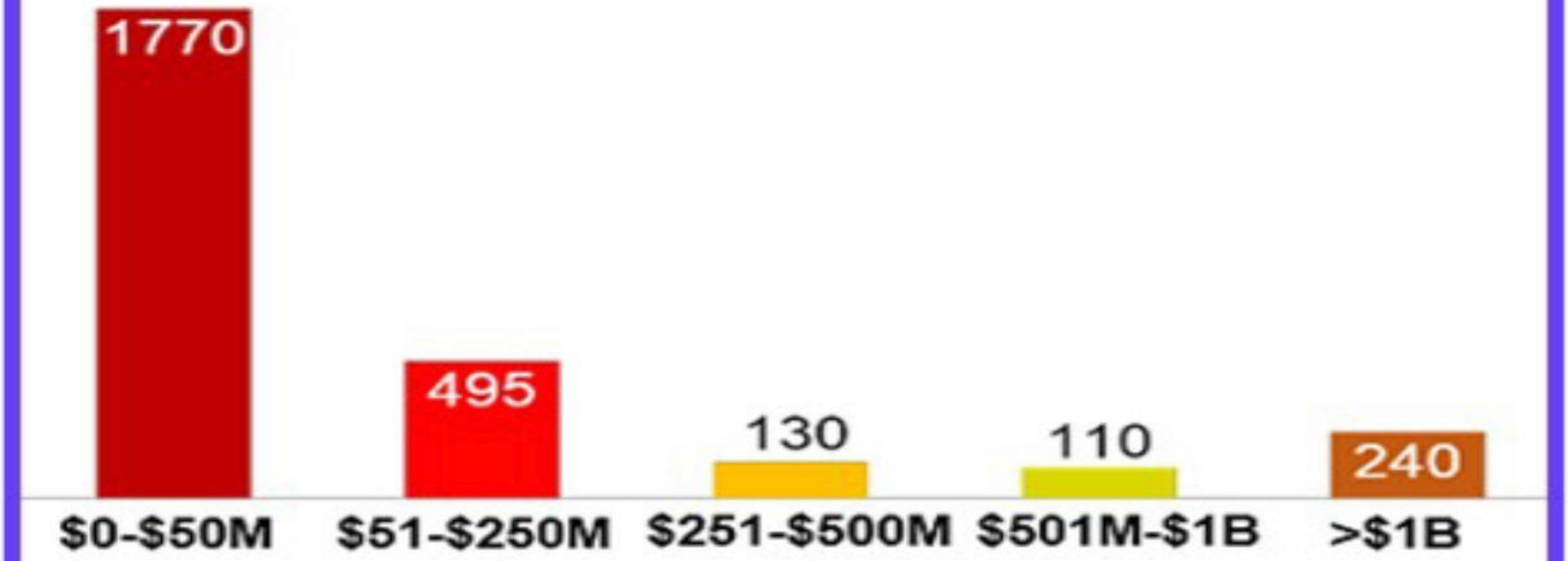
Have a problem?



Insert
End
+
=
Enter
Print Scrn
SysRq
Shift

Size of Ransom *Victims*

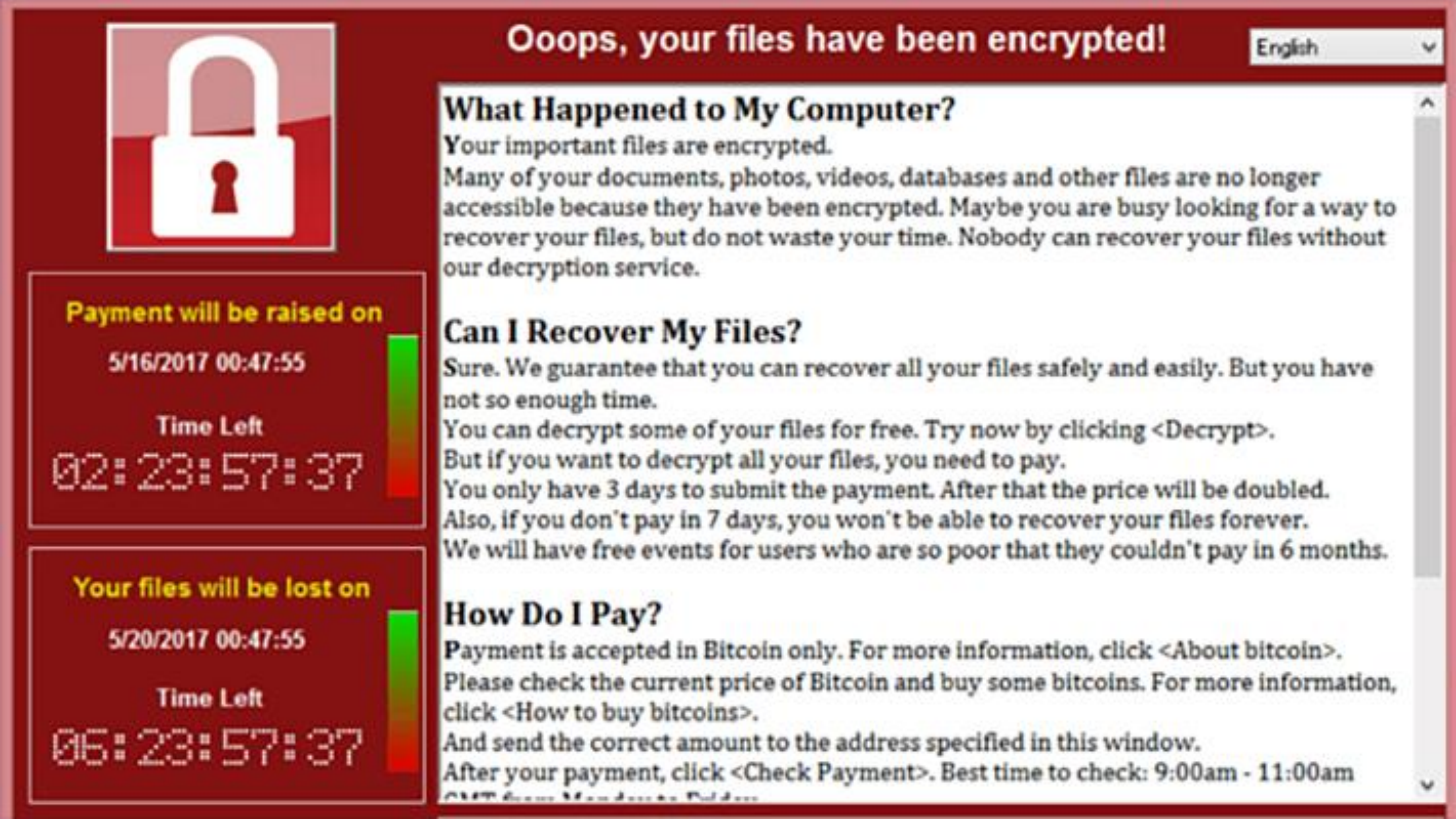
1770 of breached firms have a revenue of $0-$50M



Akamai

90 Ransom Group Leak Sites

Published August 2023



Ooops, your files have been encrypted!

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.

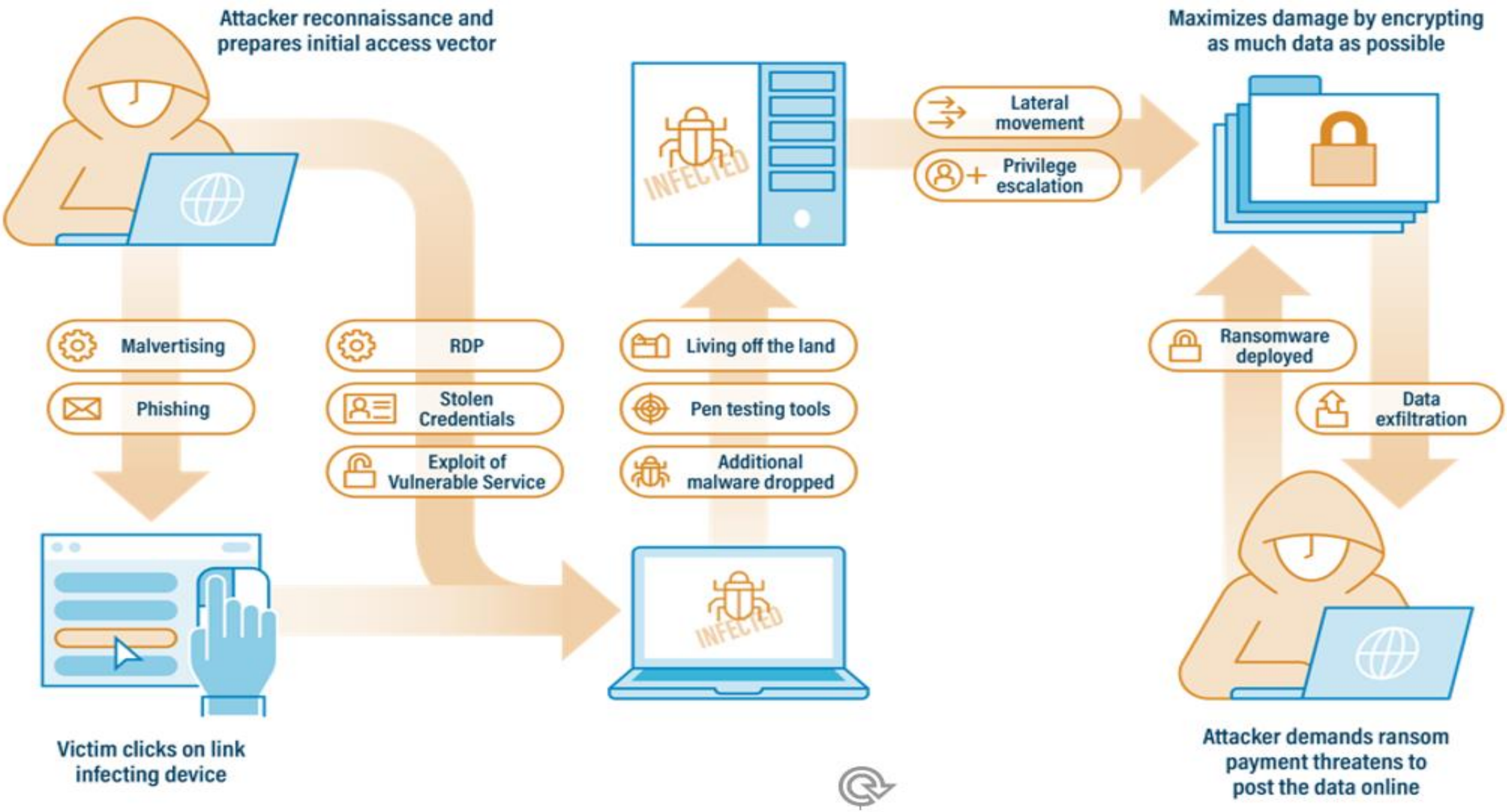
How Do I Pay?

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 GMT from Monday to Friday.



Attacker reconnaissance and prepares initial access vector

Malvertising

Phishing

Victim clicks on link infecting device

RDP

Stolen Credentials

Exploit of Vulnerable Service

INFECTED

Living off the land

Pen testing tools

Additional malware dropped

INFECTED

Lateral movement

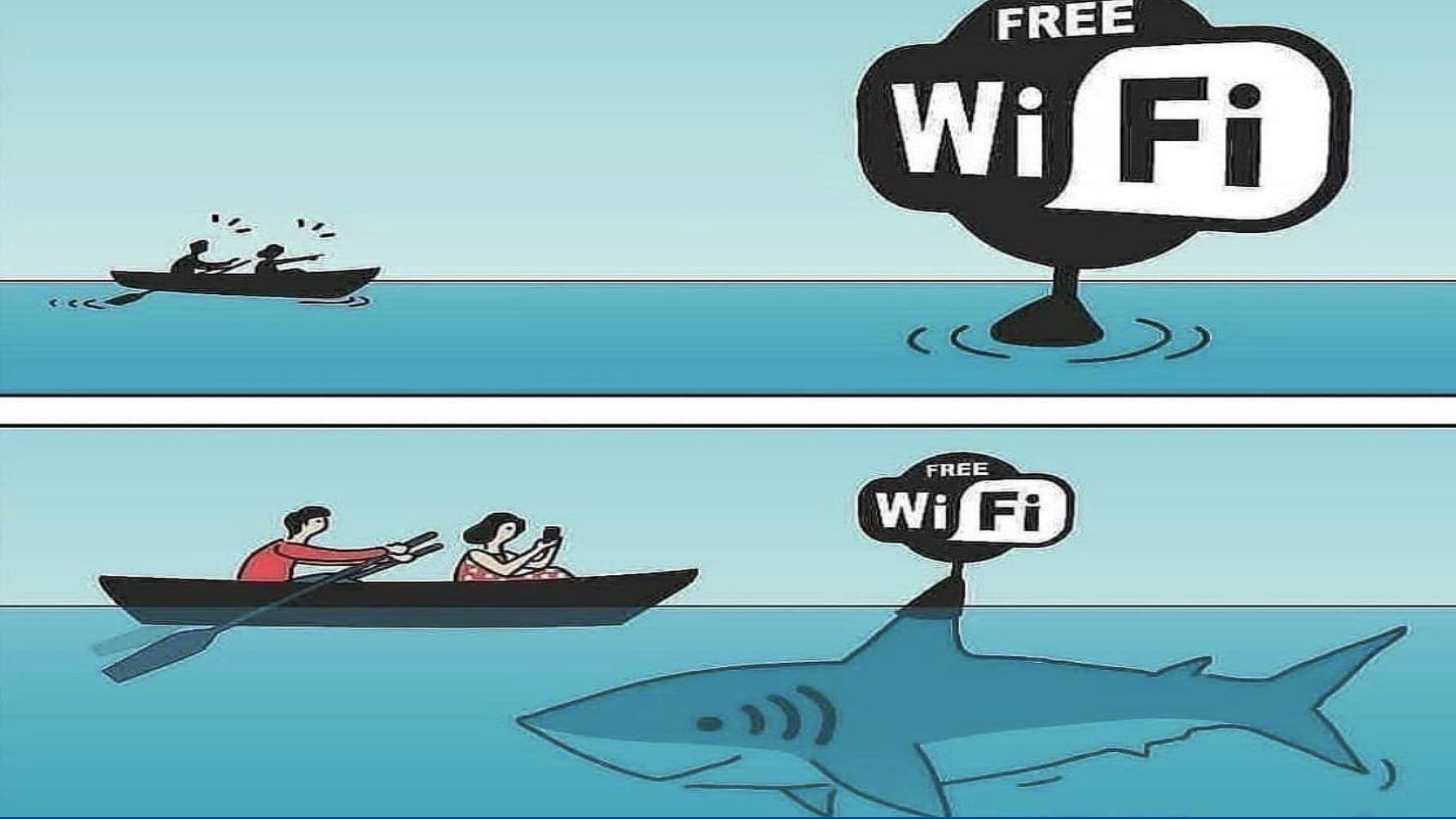
Privilege escalation

Maximizes damage by encrypting as much data as possible

Ransomware deployed

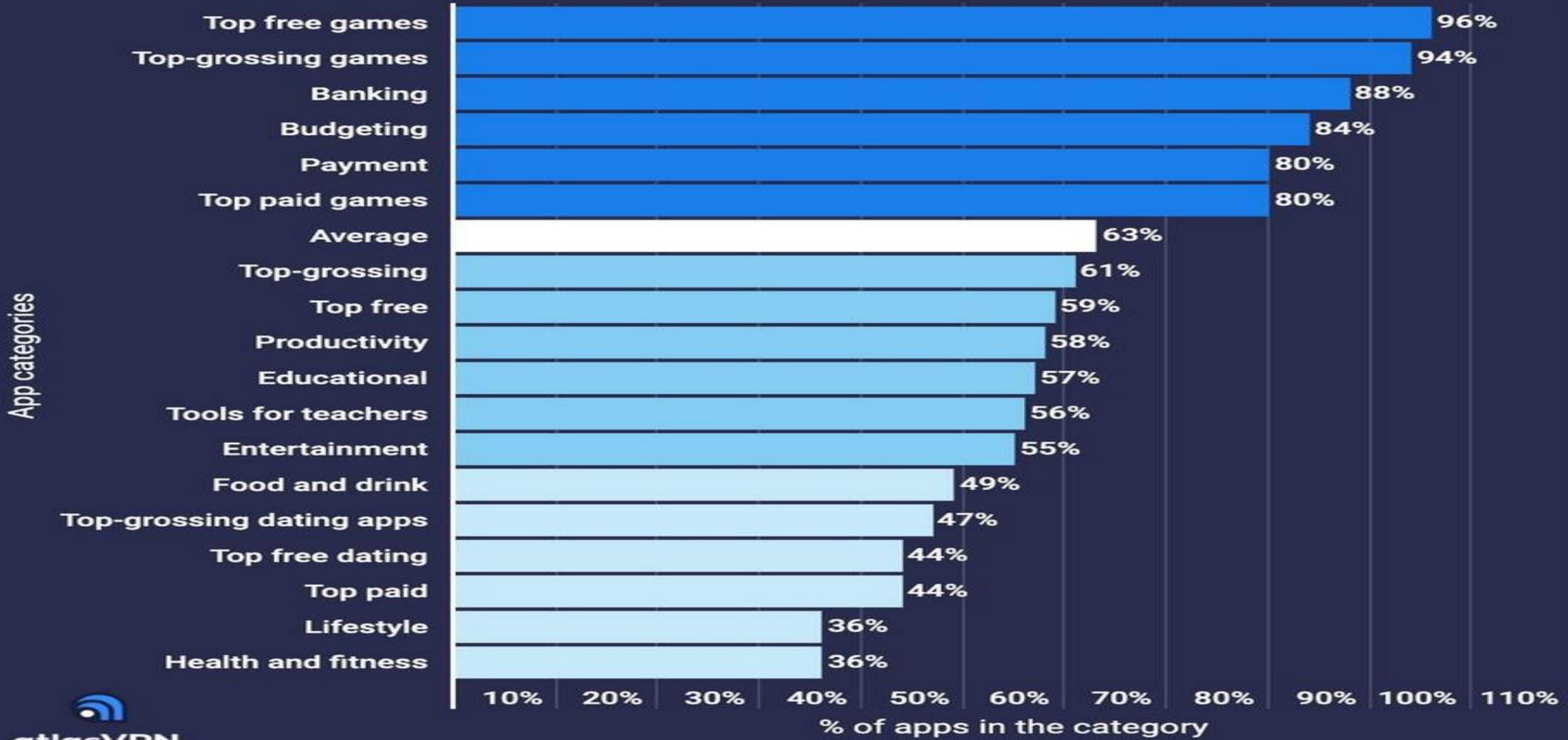
Data exfiltration

Attacker demands ransom payment threatens to post the data online

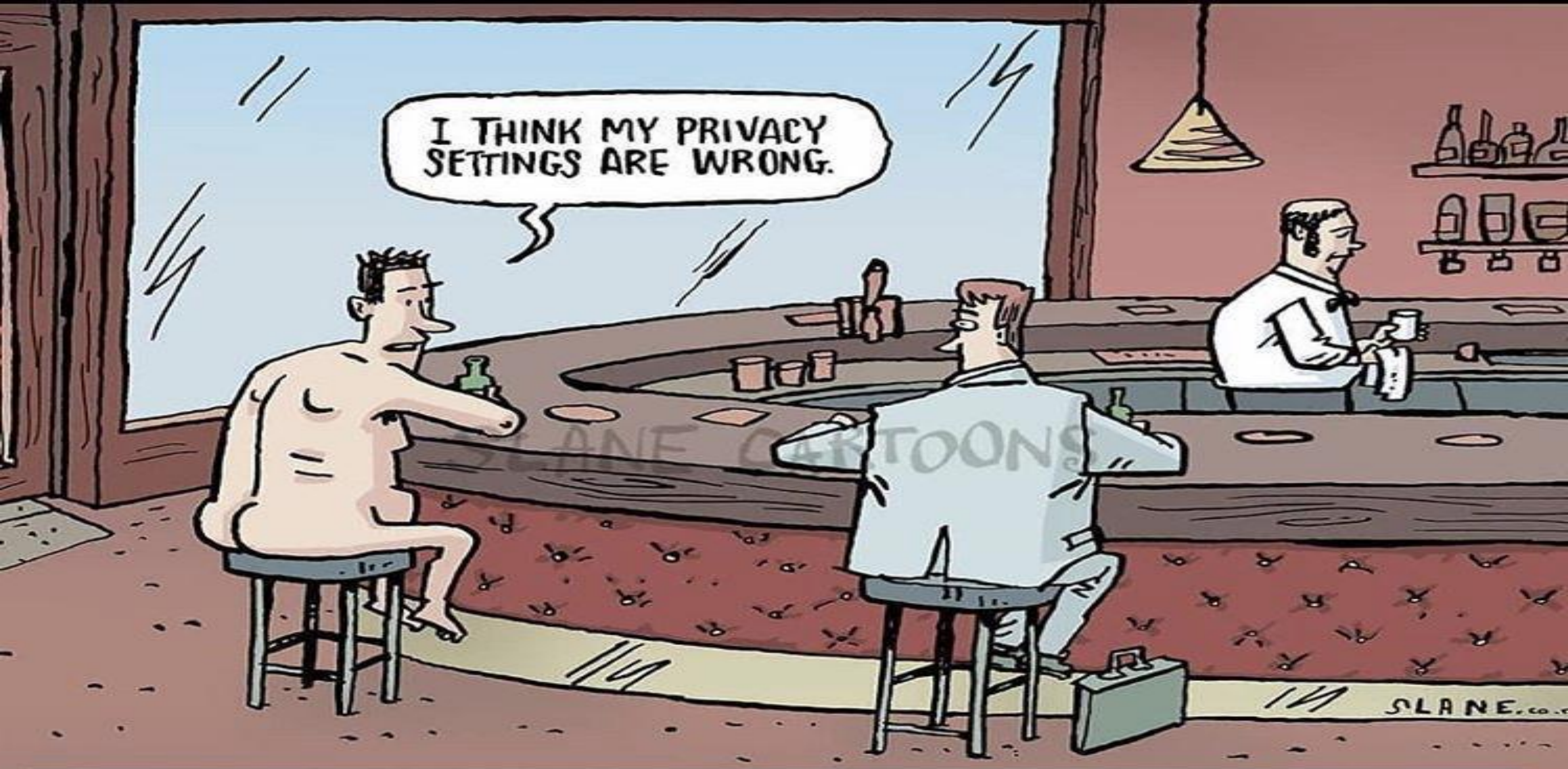

FREE
WiFi
FREE
WiFi

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.

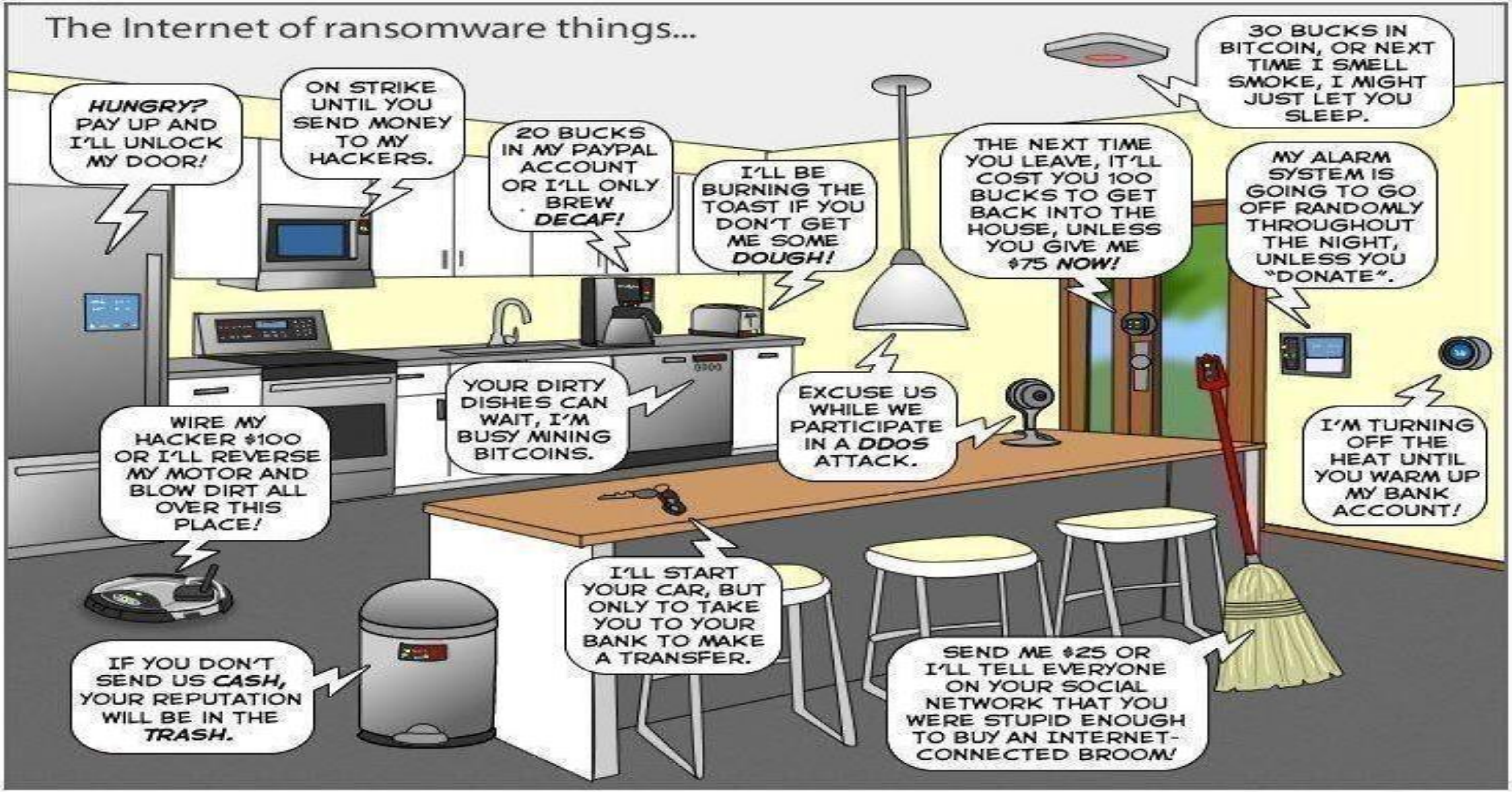


atlasVPN



ENSURE YOUR PROFILE IS SECURE ON SOCIAL MEDIA SITES.

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!

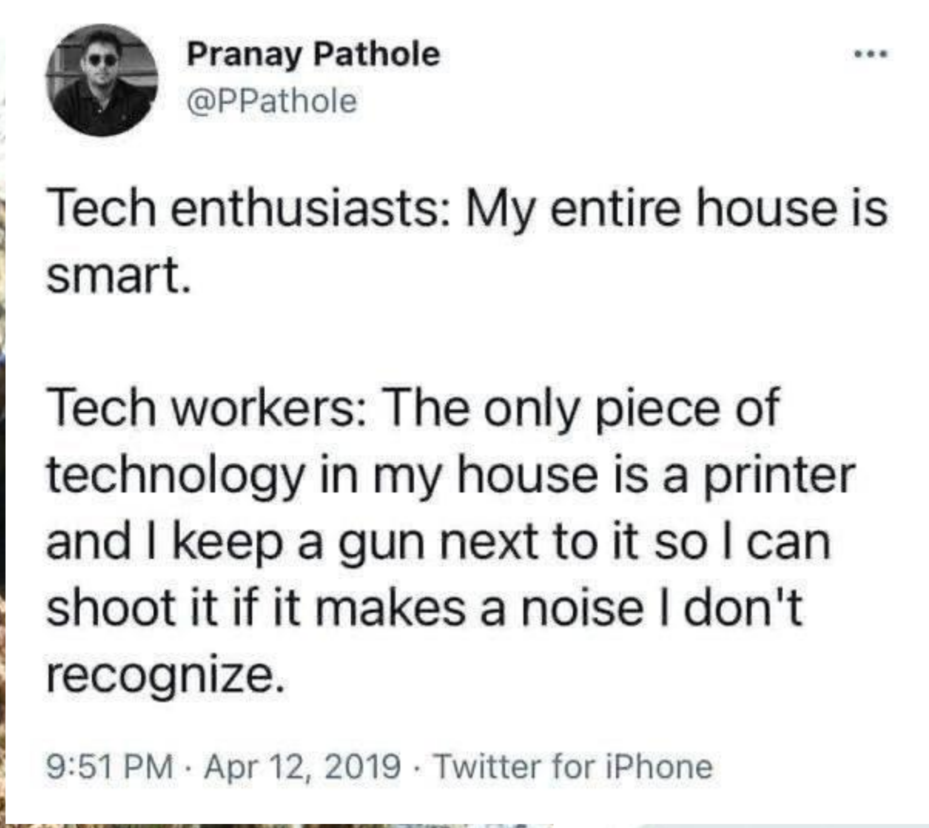
joyoftech.com

The Washington Post

Democracy Dies in Darkness

Innovations

How a fish tank helped hack a casino



Pranay Pathole
@PPathole

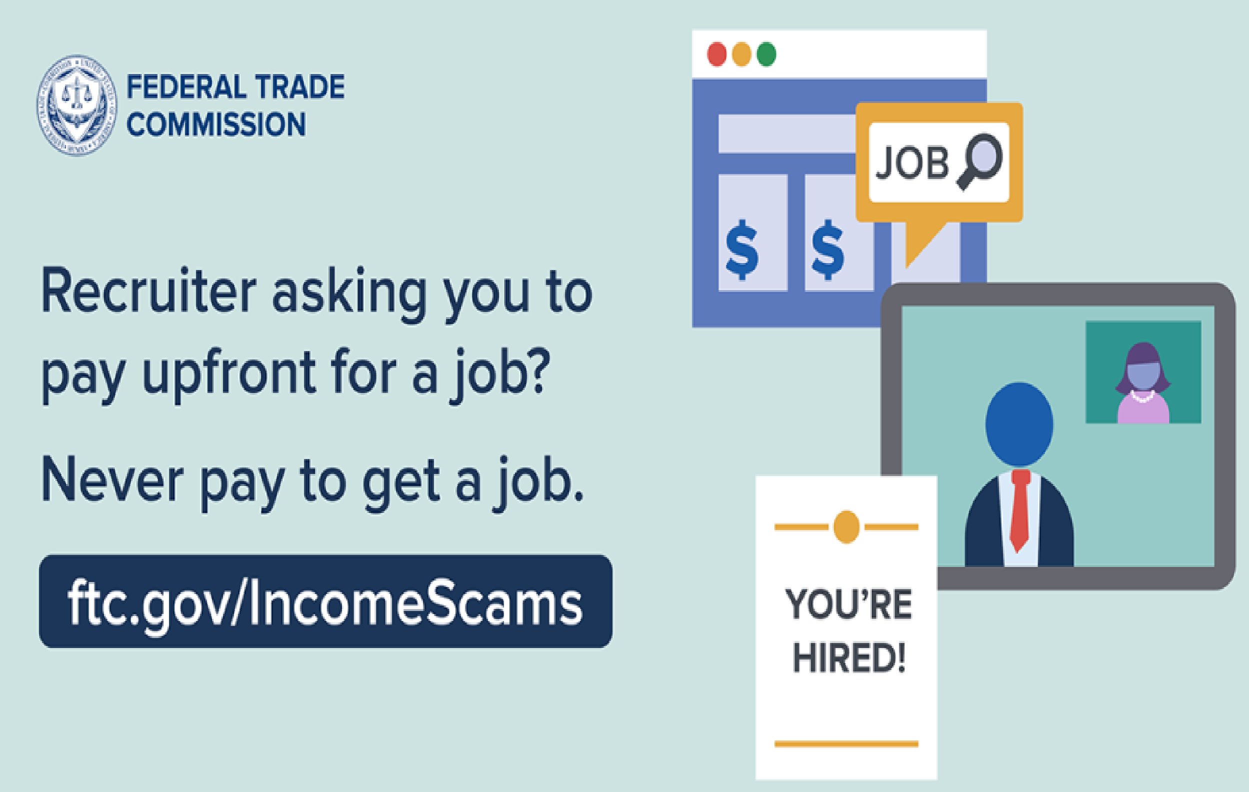
Tech enthusiasts: My entire house is smart.

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

Sale
Connected Appliances
klossner

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

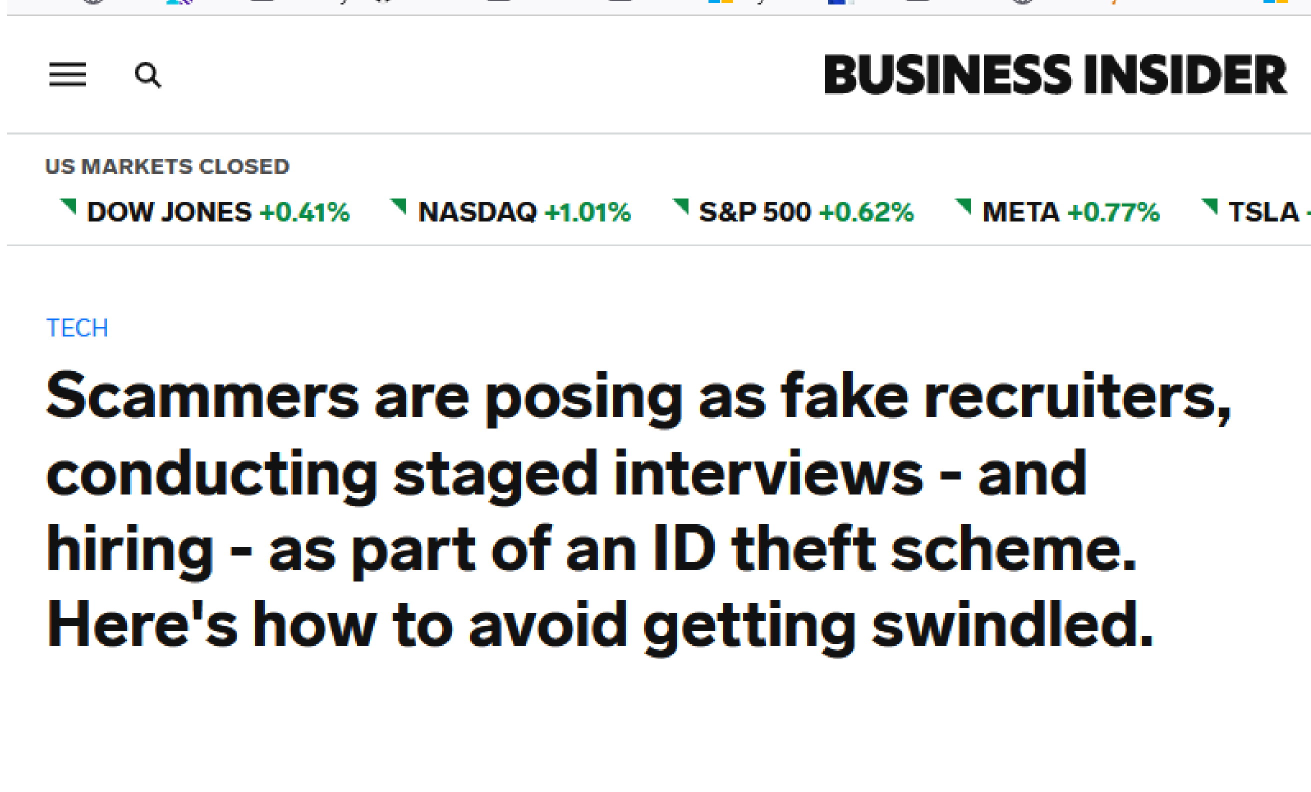


FEDERAL TRADE COMMISSION

Recruiter asking you to pay upfront for a job?

Never pay to get a job.

ftc.gov/IncomeScams



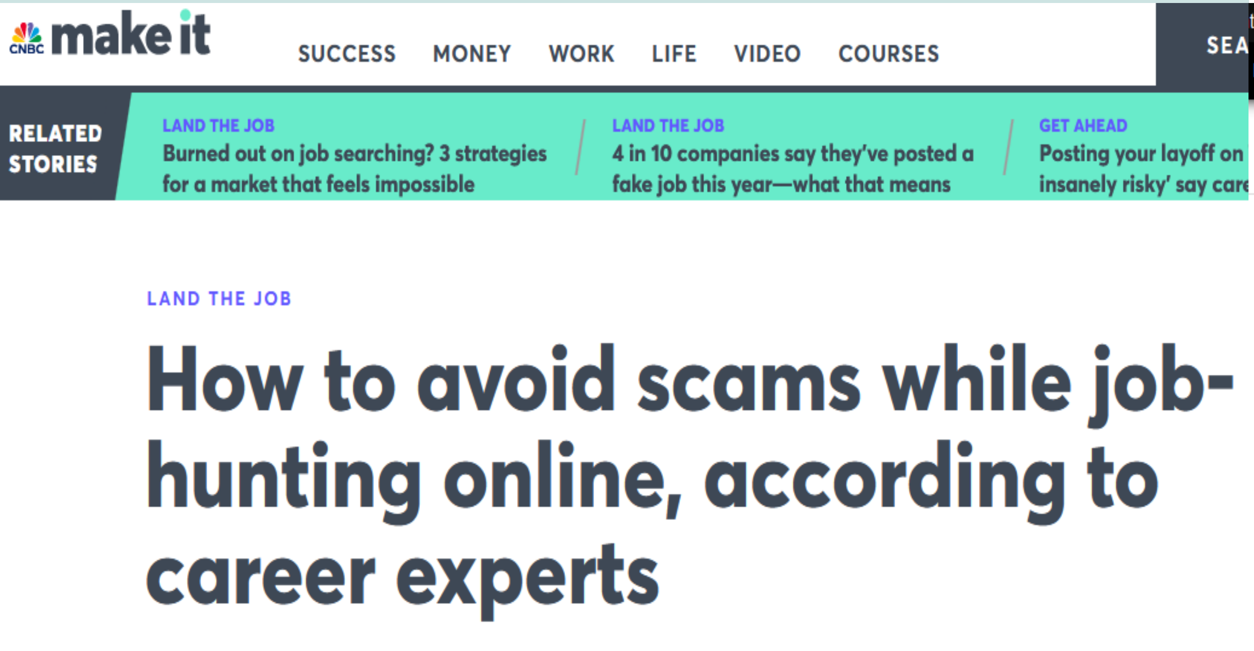
BUSINESS INSIDER

US MARKETS CLOSED

DOW JONES +0.41% NASDAQ +1.01% S&P 500 +0.62% META +0.77% TSLA

TECH

Scammers are posing as fake recruiters, conducting staged interviews - and hiring - as part of an ID theft scheme. Here's how to avoid getting swindled.



CNBC make it

SUCCESS MONEY WORK LIFE VIDEO COURSES SEA

RELATED STORIES

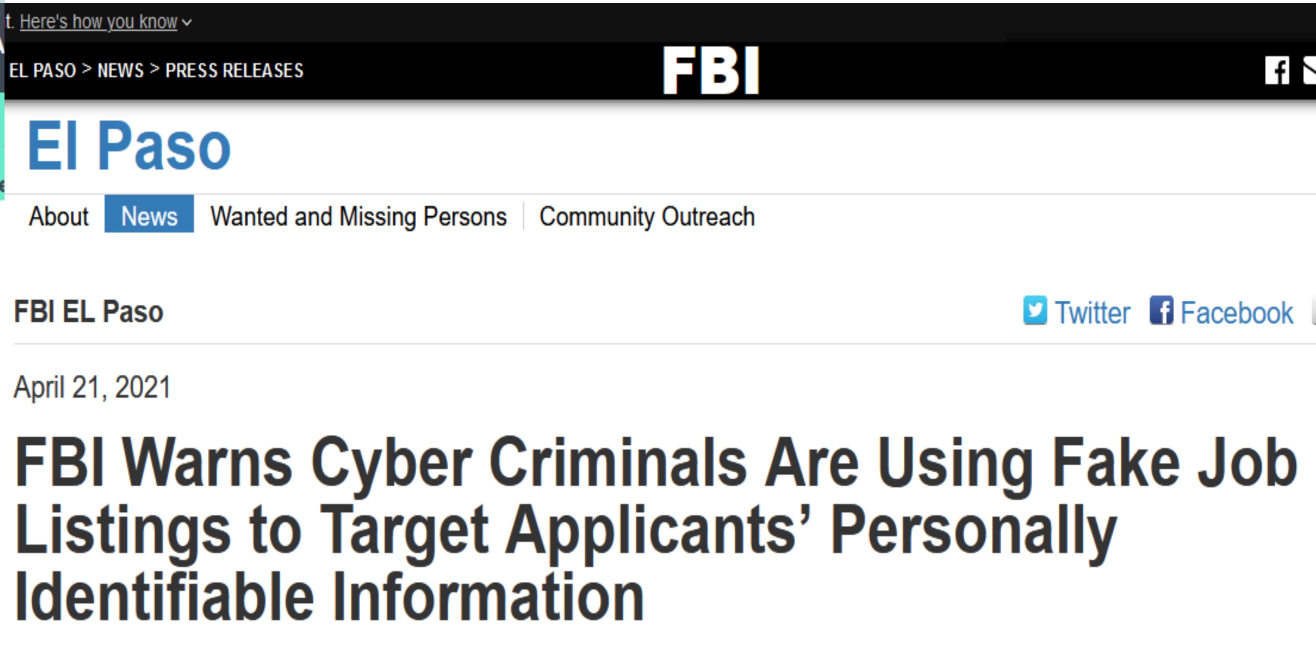
LAND THE JOB
Burned out on job searching? 3 strategies for a market that feels impossible

LAND THE JOB
4 in 10 companies say they've posted a fake job this year—what that means

GET AHEAD
Posting your layoff on insanely risky' say care

LAND THE JOB

How to avoid scams while job-hunting online, according to career experts



t. Here's how you know

EL PASO > NEWS > PRESS RELEASES

FBI

El Paso

About News Wanted and Missing Persons Community Outreach

FBI EL Paso

Twitter Facebook

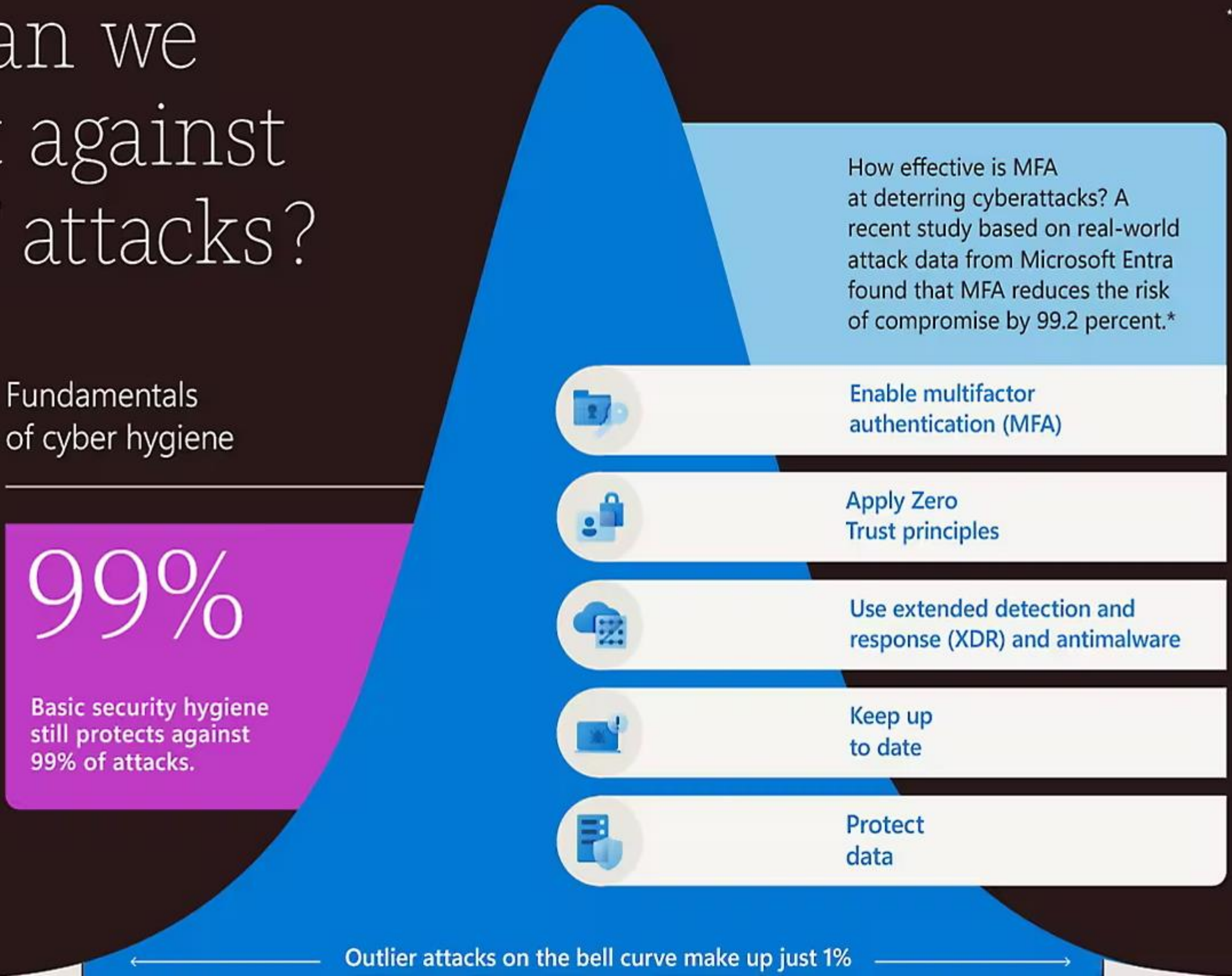
April 21, 2021

FBI Warns Cyber Criminals Are Using Fake Job Listings to Target Applicants' Personally Identifiable Information

Hope and denial are NOT a strategy!

Don’t be scared be prepared!

How can we protect against 99% of attacks?



How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.*

Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

- Enable multifactor authentication (MFA)
- Apply Zero Trust principles
- Use extended detection and response (XDR) and antimalware
- Keep up to date
- Protect data

Outlier attacks on the bell curve make up just 1%

*Source: https://arxiv.org/abs/2305.00945

Privacy <> Security

Privacy and security are different things:

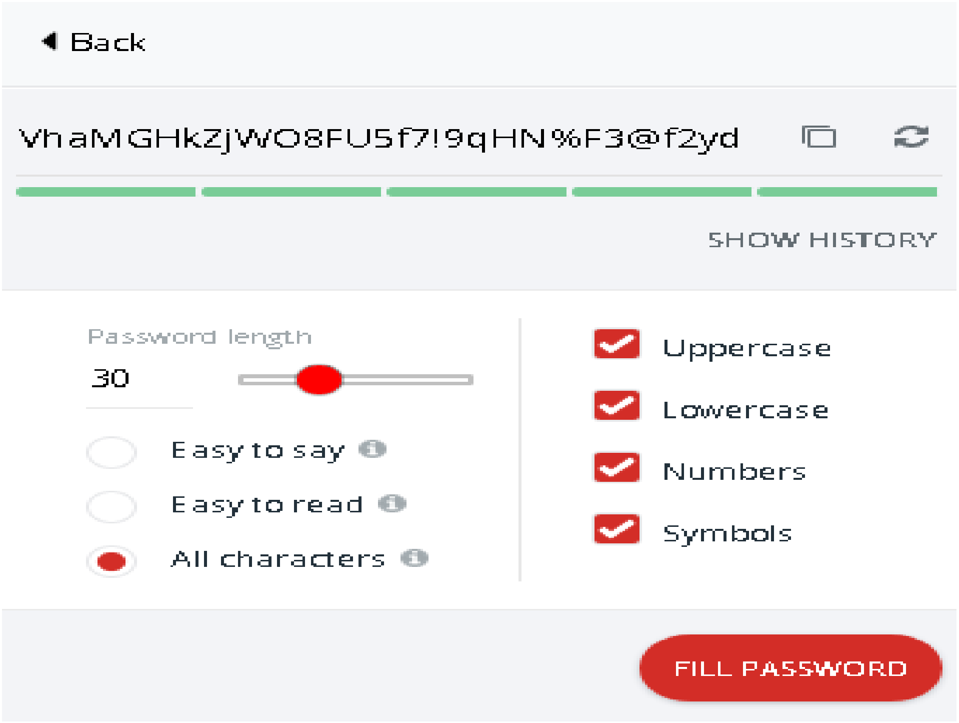
- **Security: why you lock your door**
- **Privacy: why you close your curtains**

Both are a really good idea!

Password Hygiene

- Use strong, unique passwords for *every* account
- Passphrase is better: “1l0vepizz@with0ni0ns”
- Use a password manager with MFA

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

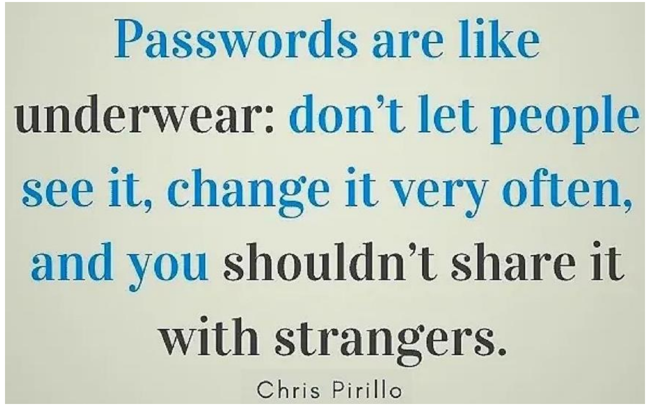


VhaMGHkZjWO8FU5f7!9qHN%F3@f2yd

Password length
30

○ Easy to say
○ Easy to read
● All characters

☑ Uppercase
☑ Lowercase
☑ Numbers
☑ Symbols

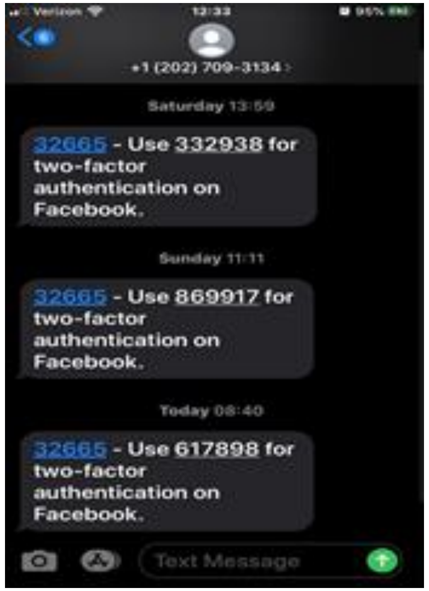


Passwords are like underwear: don’t let people see it, change it very often, and you shouldn’t share it with strangers.

Chris Pirillo

Multi-factor Authentication (MFA)

- Aka Two-factor Authentication (2FA) or Two-Step Verification
- Enable MFA everywhere
- Use an authenticator app rather than SMS based OTPs



Saturday 13:59

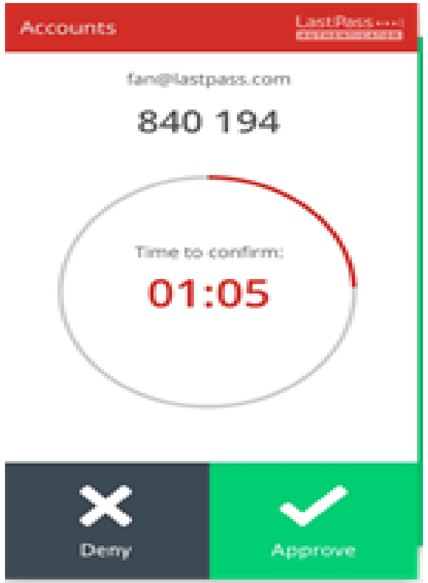
32665 - Use 332938 for two-factor authentication on Facebook.

Sunday 11:11

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

Today 08:40

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



fan@lastpass.com

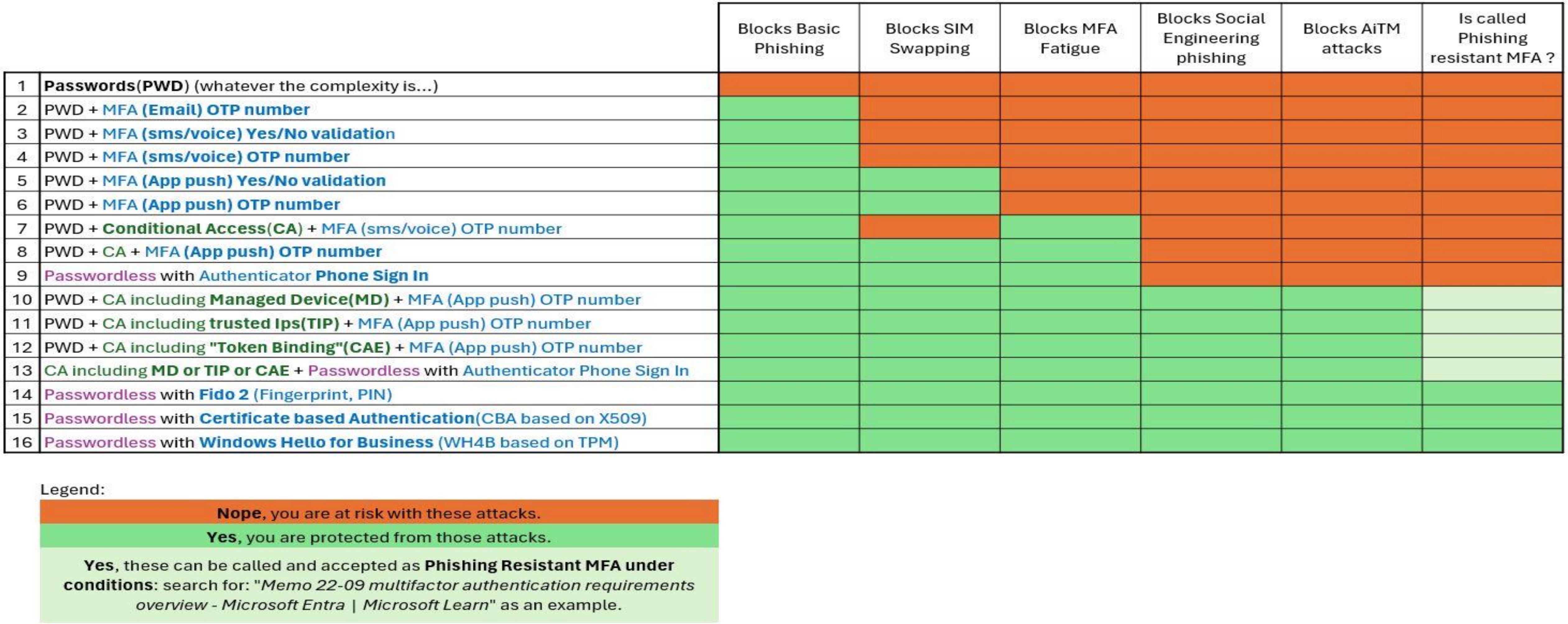
840 194

Time to confirm:

01:05

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

MFA Protection



		Blocks Basic Phishing	Blocks SIM Swapping	Blocks MFA Fatigue	Blocks Social Engineering phishing	Blocks AiTM attacks	Is called Phishing resistant MFA ?
1	**Passwords**(**PWD**) (whatever the complexity is...)	🟥	🟥	🟥	🟥	🟥	🟥
2	PWD + MFA **(Email) OTP number**	🟩	🟥	🟥	🟥	🟥	🟥
3	PWD + MFA **(sms/voice) Yes/No validation**	🟩	🟥	🟥	🟥	🟥	🟥
4	PWD + MFA **(sms/voice) OTP number**	🟩	🟥	🟥	🟥	🟥	🟥
5	PWD + MFA **(App push) Yes/No validation**	🟩	🟩	🟥	🟥	🟥	🟥
6	PWD + MFA **(App push) OTP number**	🟩	🟩	🟥	🟥	🟥	🟥
7	PWD + **Conditional Access**(**CA**) + MFA (sms/voice) OTP number	🟩	🟥	🟩	🟥	🟥	🟥
8	PWD + CA + MFA **(App push) OTP number**	🟩	🟩	🟩	🟥	🟥	🟥
9	Passwordless with Authenticator **Phone Sign In**	🟩	🟩	🟩	🟥	🟥	🟥
10	PWD + CA including **Managed Device(MD)** + MFA (App push) OTP number	🟩	🟩	🟩	🟩	🟩	🟢
11	PWD + CA including **trusted Ips(TIP)** + MFA (App push) OTP number	🟩	🟩	🟩	🟩	🟩	🟢
12	PWD + CA including **"Token Binding"(CAE)** + MFA (App push) OTP number	🟩	🟩	🟩	🟩	🟩	🟢
13	CA including **MD or TIP or CAE** + Passwordless with Authenticator Phone Sign In	🟩	🟩	🟩	🟩	🟩	🟢
14	Passwordless with **Fido 2** (Fingerprint, PIN)	🟩	🟩	🟩	🟩	🟩	🟩
15	Passwordless with **Certificate based Authentication**(CBA based on X509)	🟩	🟩	🟩	🟩	🟩	🟩
16	Passwordless with **Windows Hello for Business** (WH4B based on TPM)	🟩	🟩	🟩	🟩	🟩	🟩

Legend:

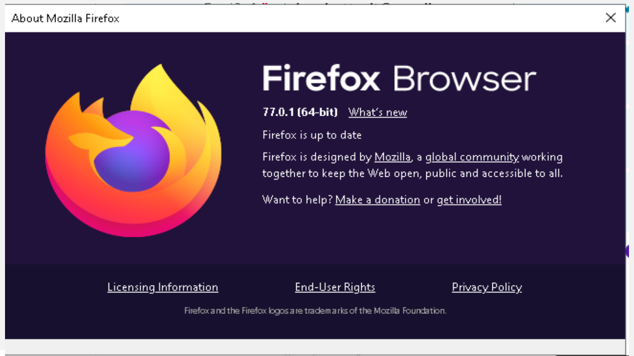
🟥 **Nope**, you are at risk with these attacks.

🟩 **Yes**, you are protected from those attacks.

🟢 **Yes**, these can be called and accepted as **Phishing Resistant MFA under conditions**: search for: "*Memo 22-09 multifactor authentication requirements overview - Microsoft Entra | Microsoft Learn*" as an example.

Software updates

- *ALL* devices that contain software!
- Automate



About Mozilla Firefox

Firefox Browser

77.0.1 (64-bit) What's new

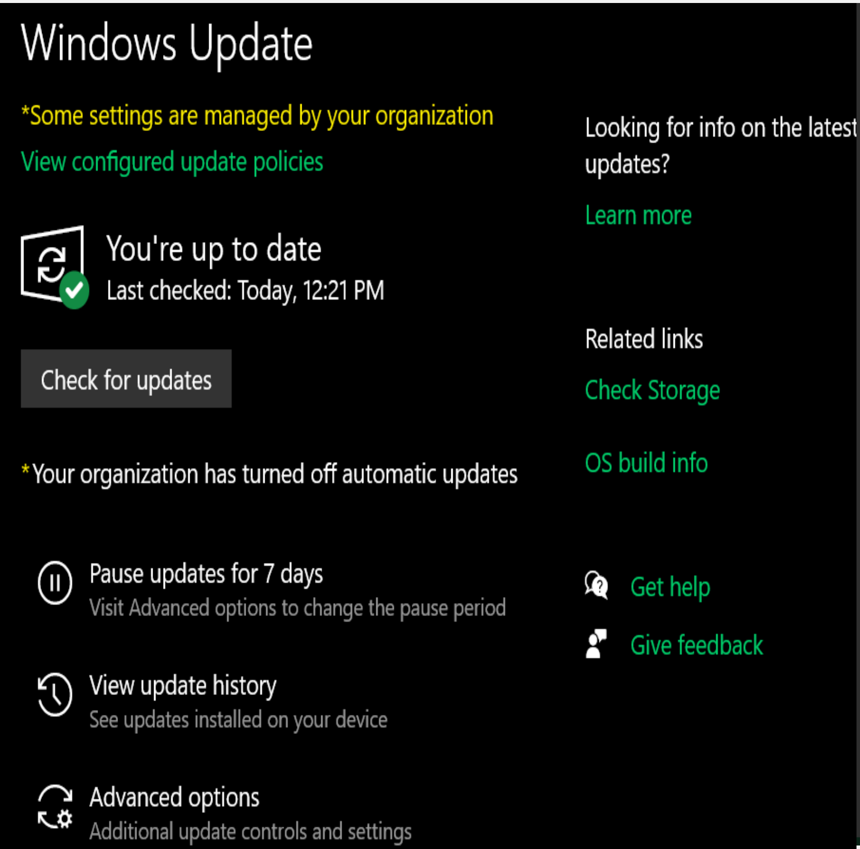
Firefox is up to date

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.



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

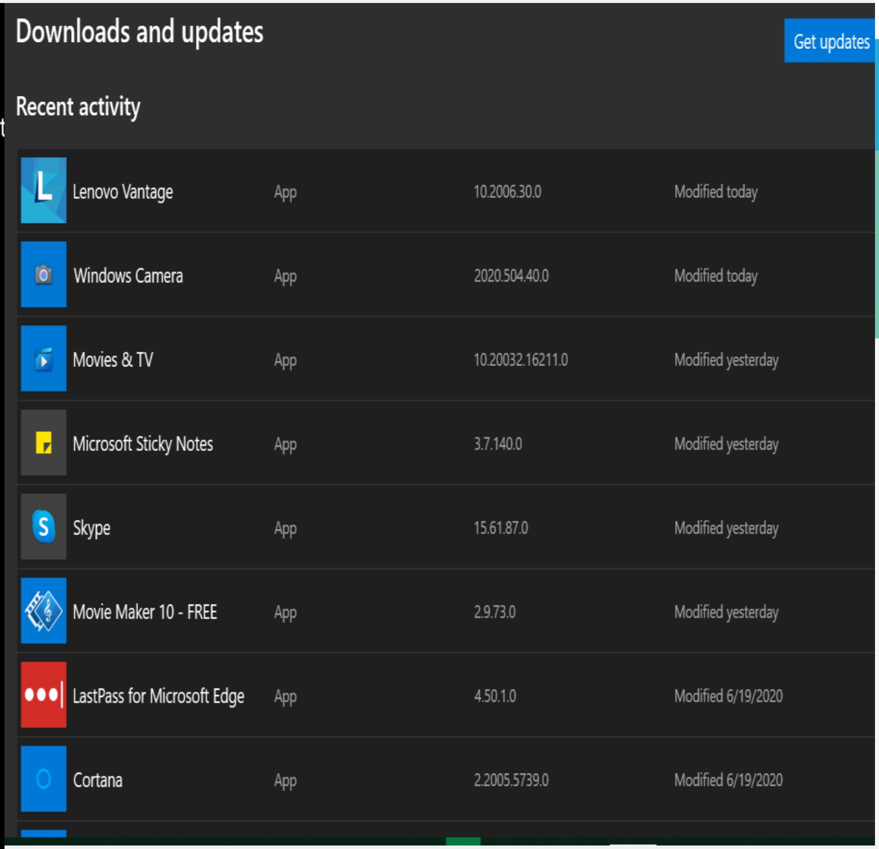
Related links

Check Storage

OS build info

Get help

Give feedback

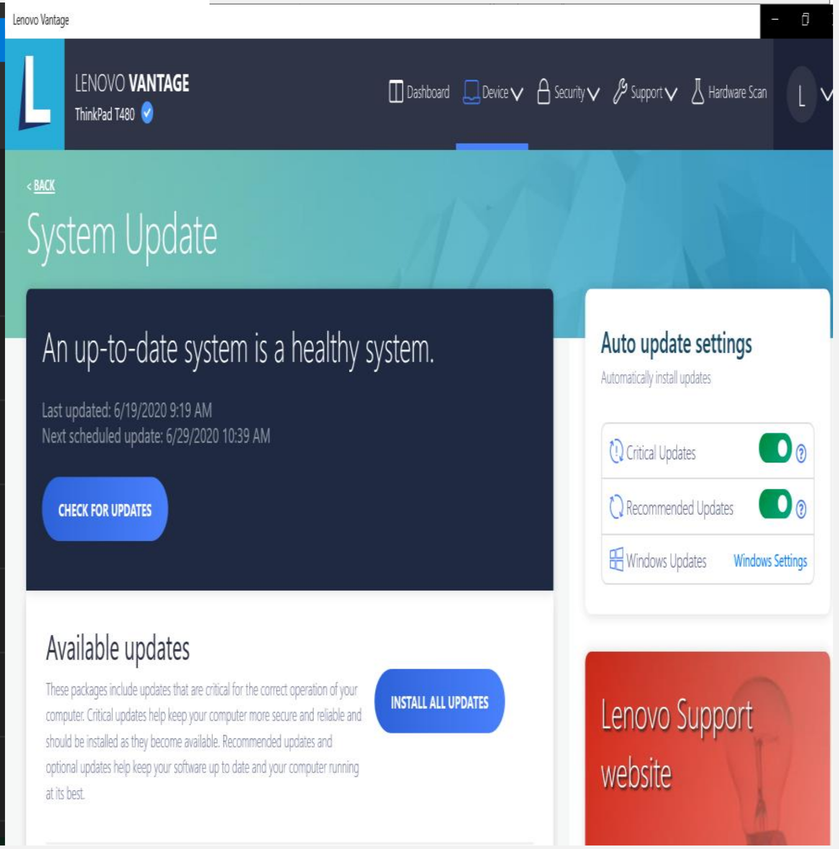


Downloads and updates

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



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

Auto update settings

Automatically install updates

Critical Updates ●
Recommended Updates ●
Windows Updates — Windows Settings

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.

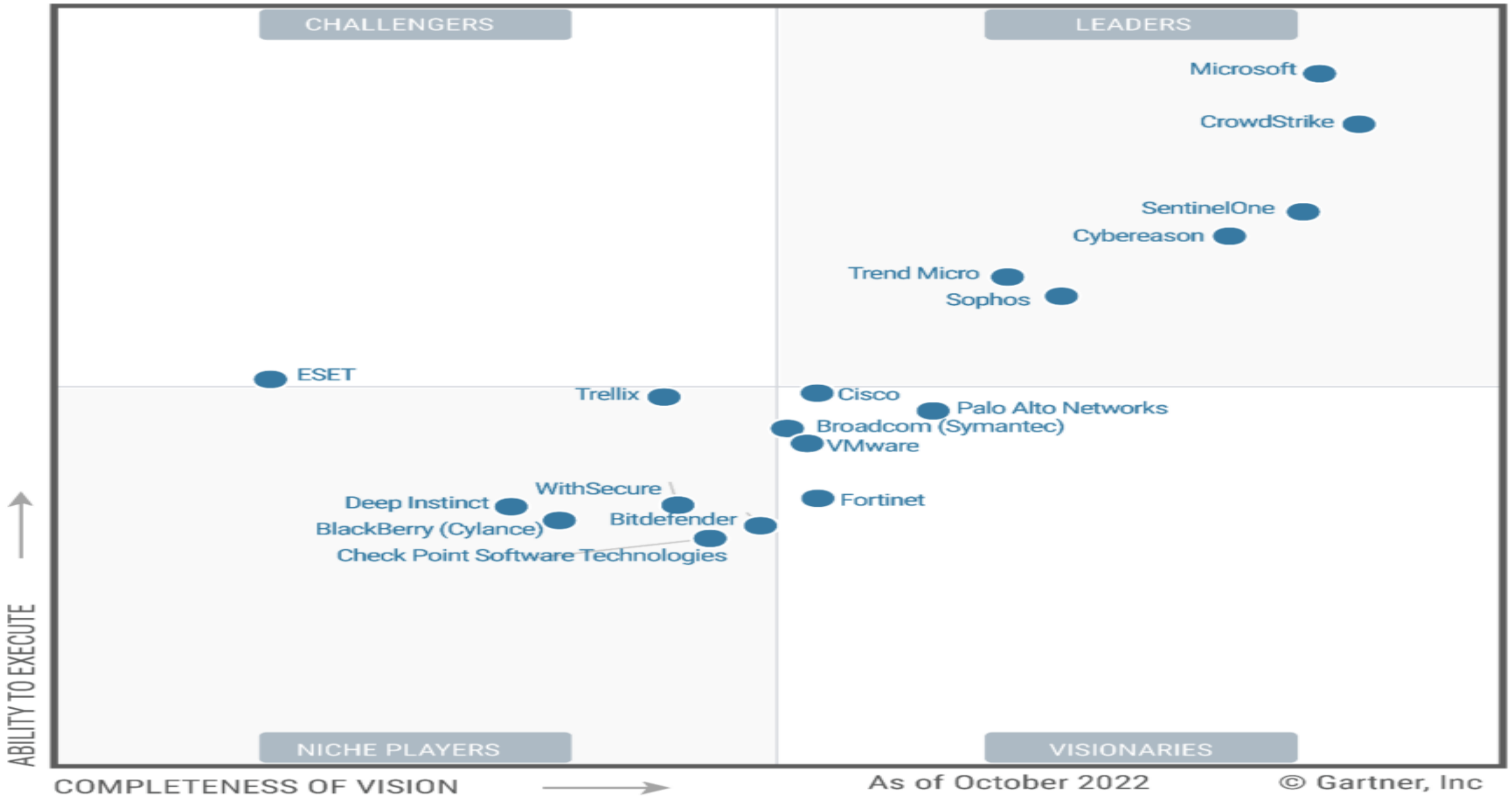
INSTALL ALL UPDATES

Lenovo Support website

Endpoint Protection (EPP)

- AKA anti-malware, anti-virus, MDR, EDR, XDR
- Update!

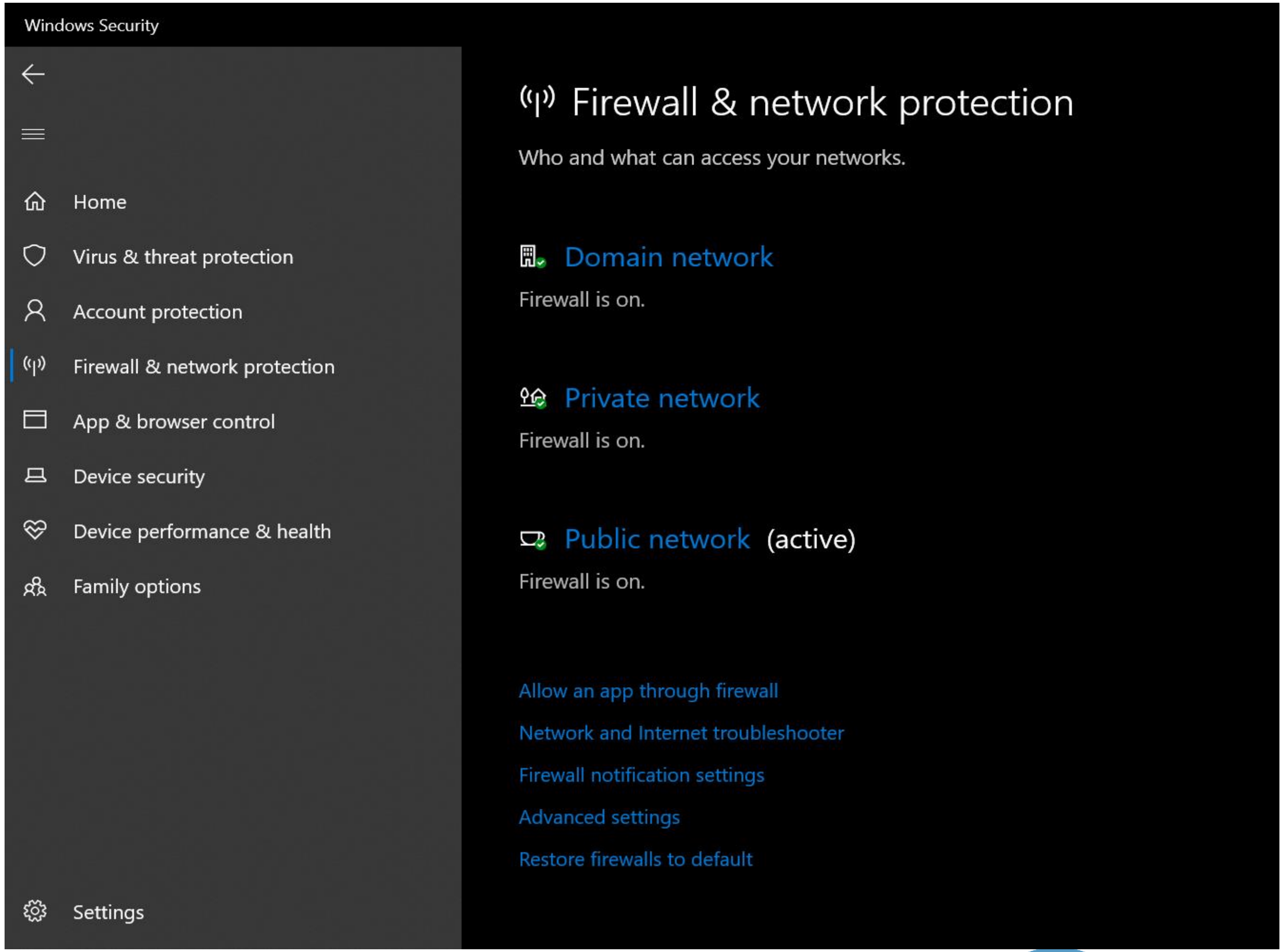
Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (December 2022)

Firewall

- Use a firewall to protect your device / network
- Your router can be configured to act as a firewall
- Windows has 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.

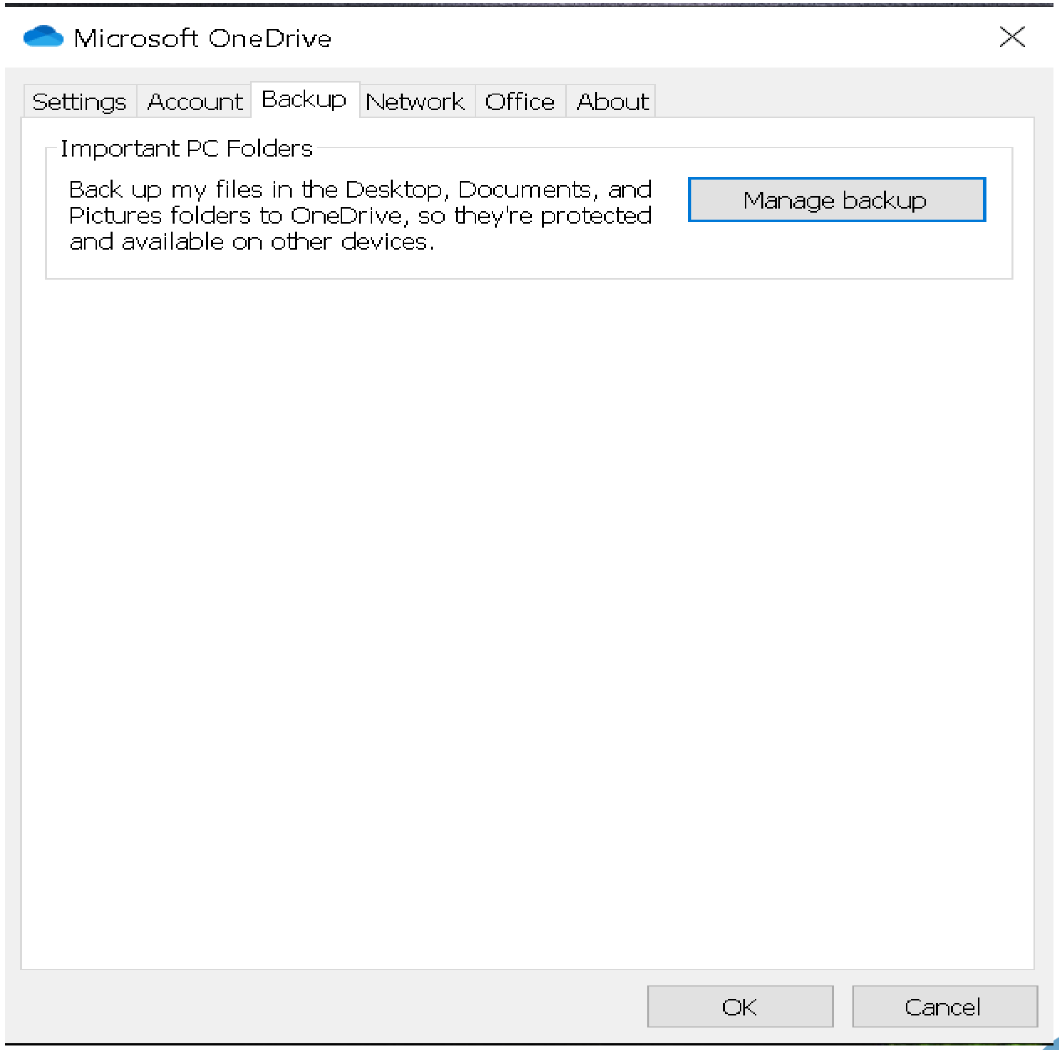
Public network (active)

Firewall is on.

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

Backup

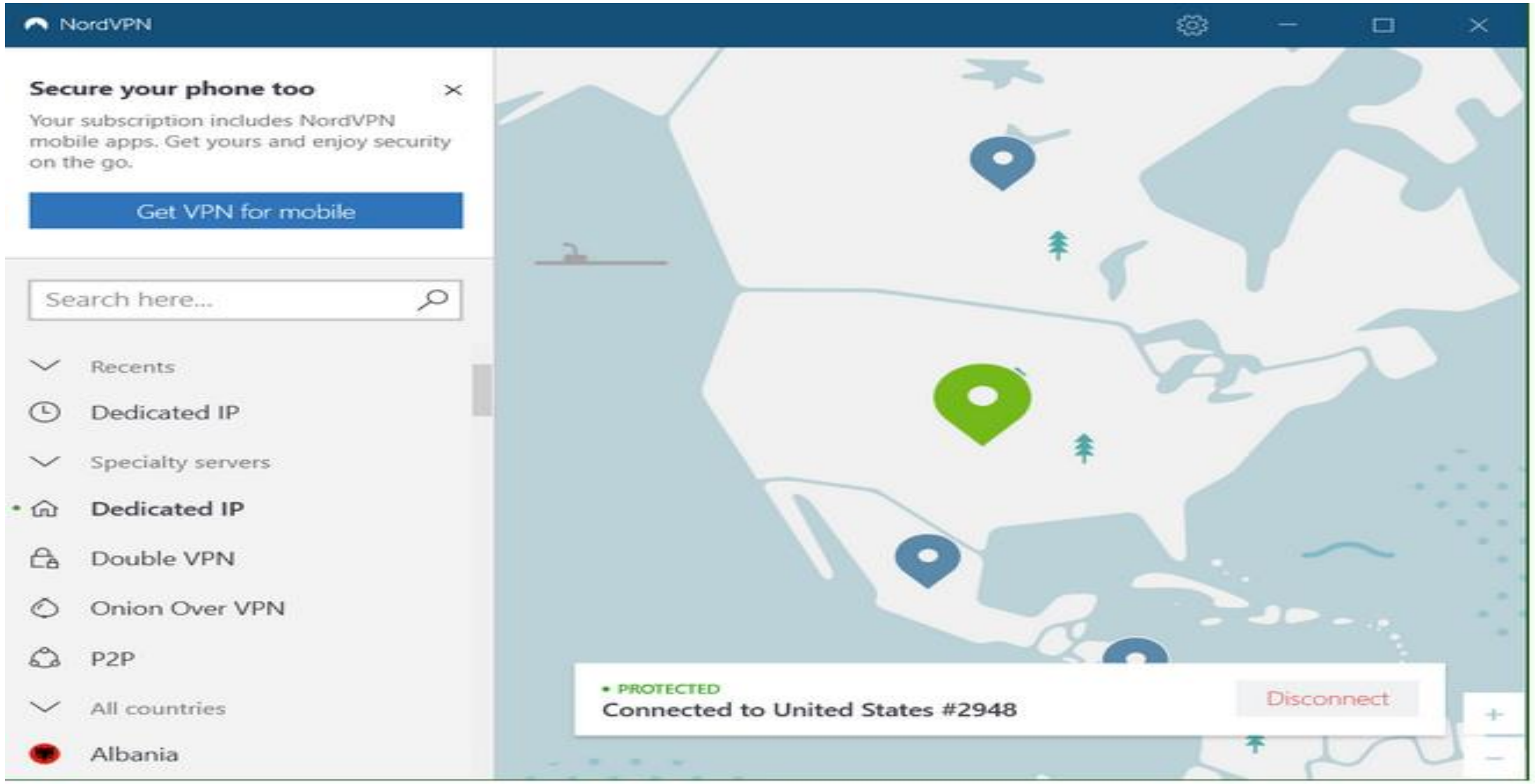
- 3-2-1 rule
  - At least 3 versions of your data on two different media, one of which is off-site
- Test backups!



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

Virtual Private Network (VPN)

- Create an encrypted connection
- Never use public Wi-Fi without a VPN
- Less critical if all your apps are cloud based

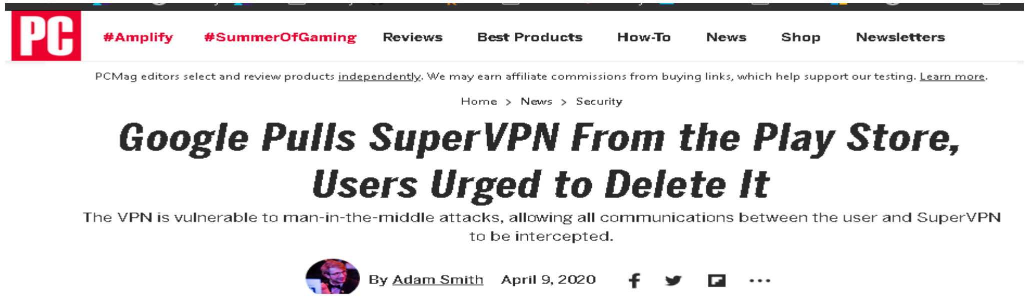


Secure your phone too

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

• 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

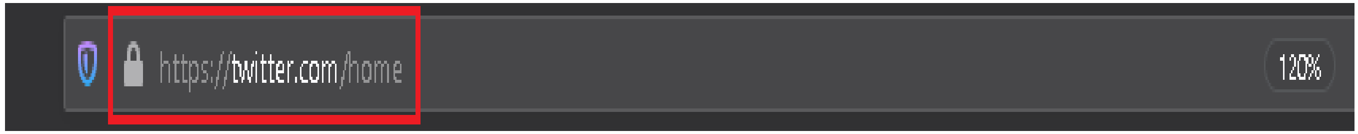
Google Pulls SuperVPN From the Play Store, Users Urged to Delete It

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

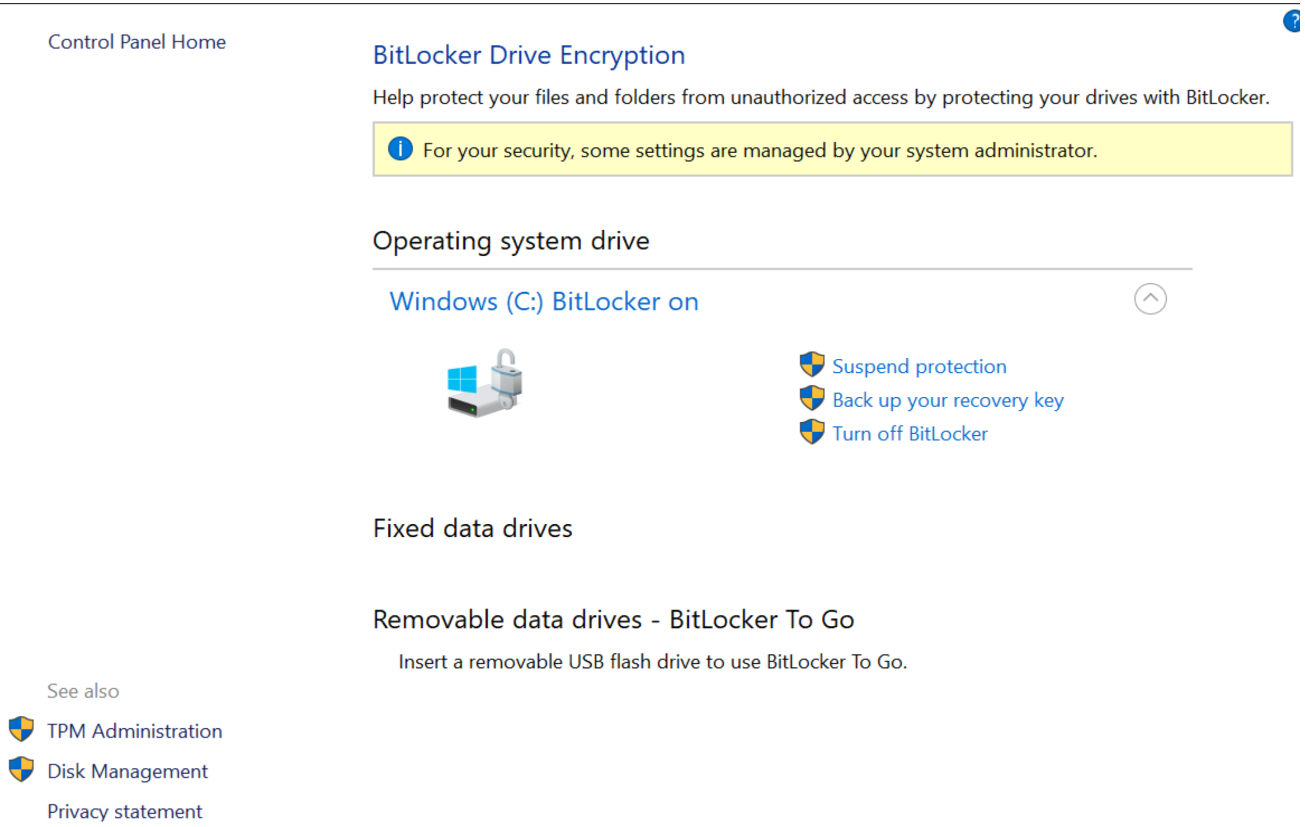
Encryption

- Scrambles data so that it can only be unscrambled with the appropriate key



https://twitter.com/home

- Encrypt data at rest and in transit



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

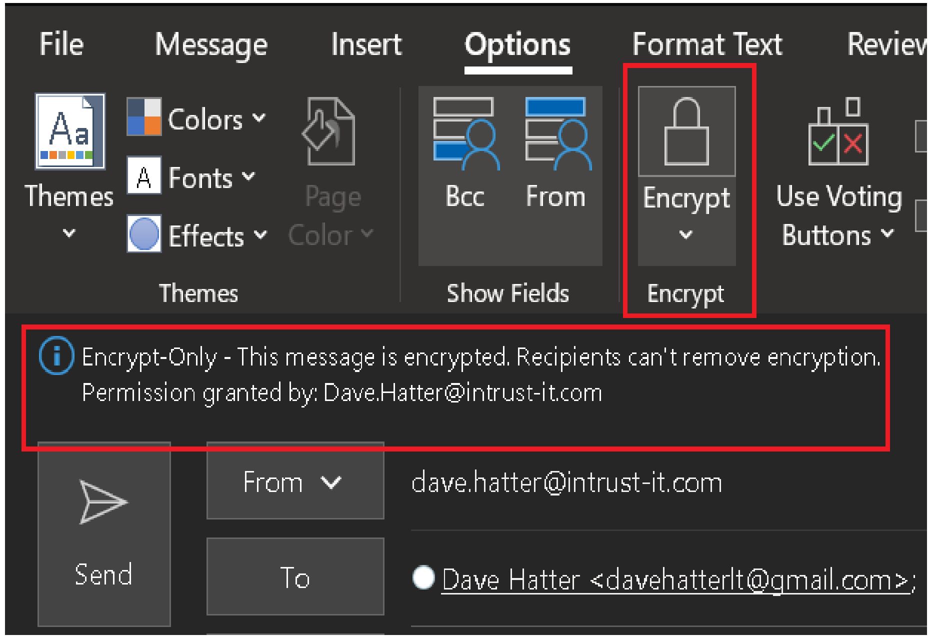
Insert a removable USB flash drive to use BitLocker To Go.

See also

TPM Administration

Disk Management

Privacy statement



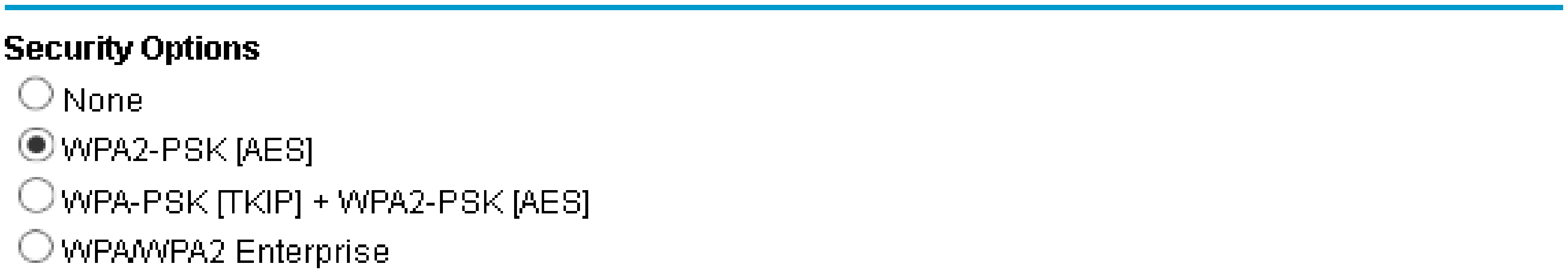
ⓘ Encrypt-Only - This message is encrypted. Recipients can't remove encryption.
Permission granted by: Dave.Hatter@intrust-it.com

From: dave.hatter@intrust-it.com

To: Dave Hatter <davehatterlt@gmail.com>;

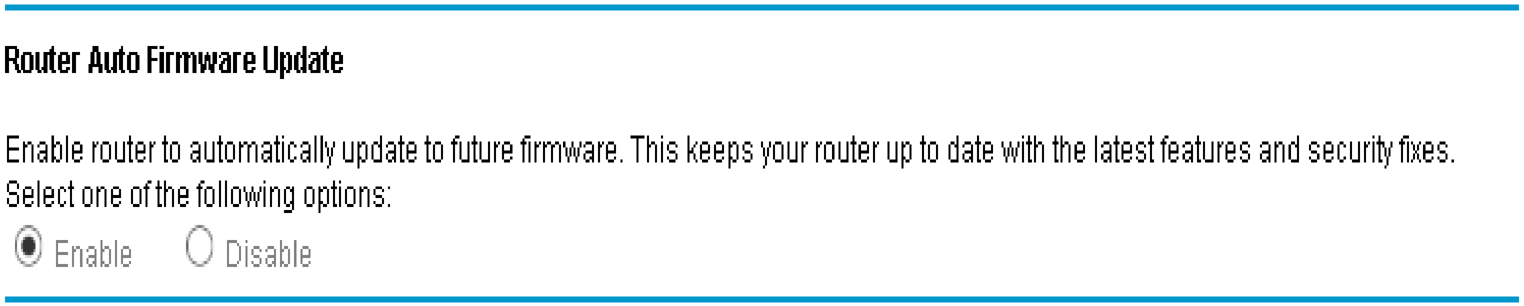
Wi-Fi

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



Security Options

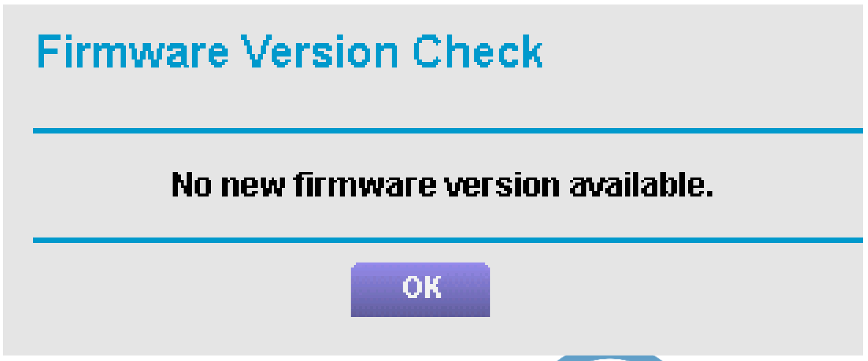
○ None
● WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]
○ WPA/WPA2 Enterprise



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

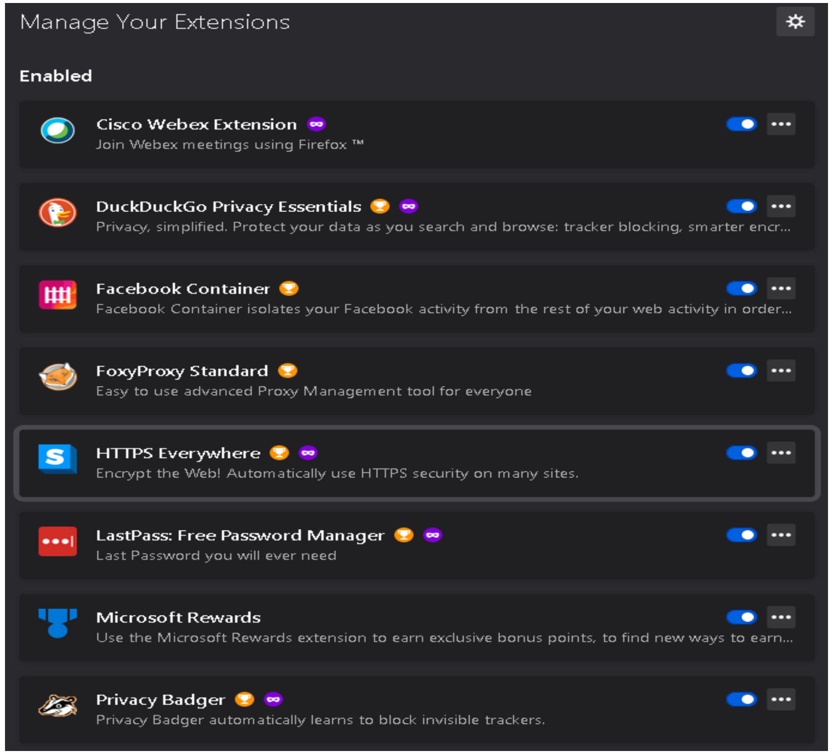


Firmware Version Check

No new firmware version available.

Vet software carefully

- 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...

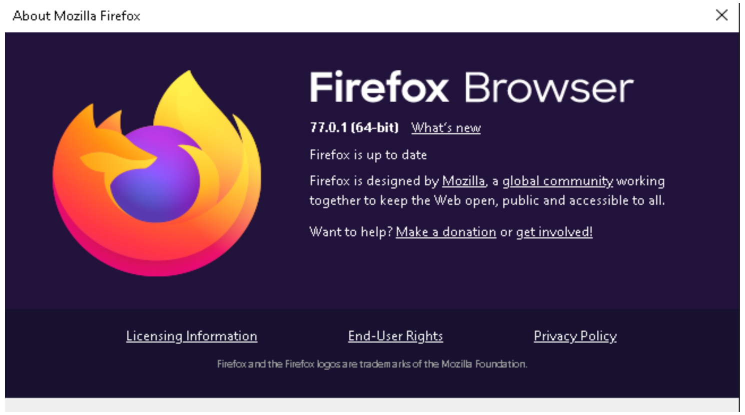
FoxyProxy Standard
Easy to use advanced Proxy Management tool for everyone

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 Mozilla Firefox

Firefox Browser

77.0.1 (64-bit) What's new

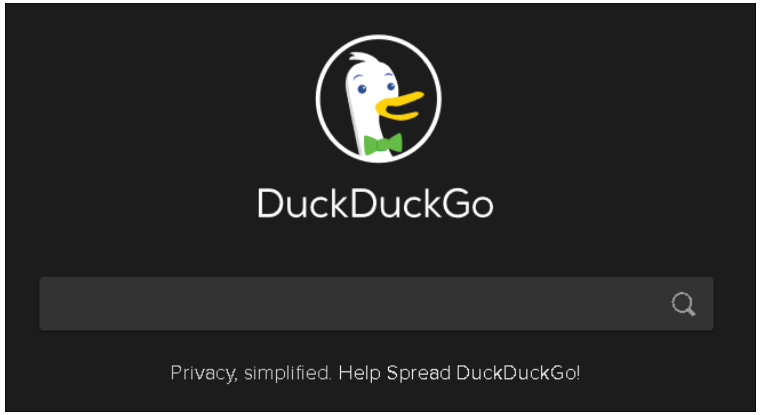
Firefox is up to date

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!

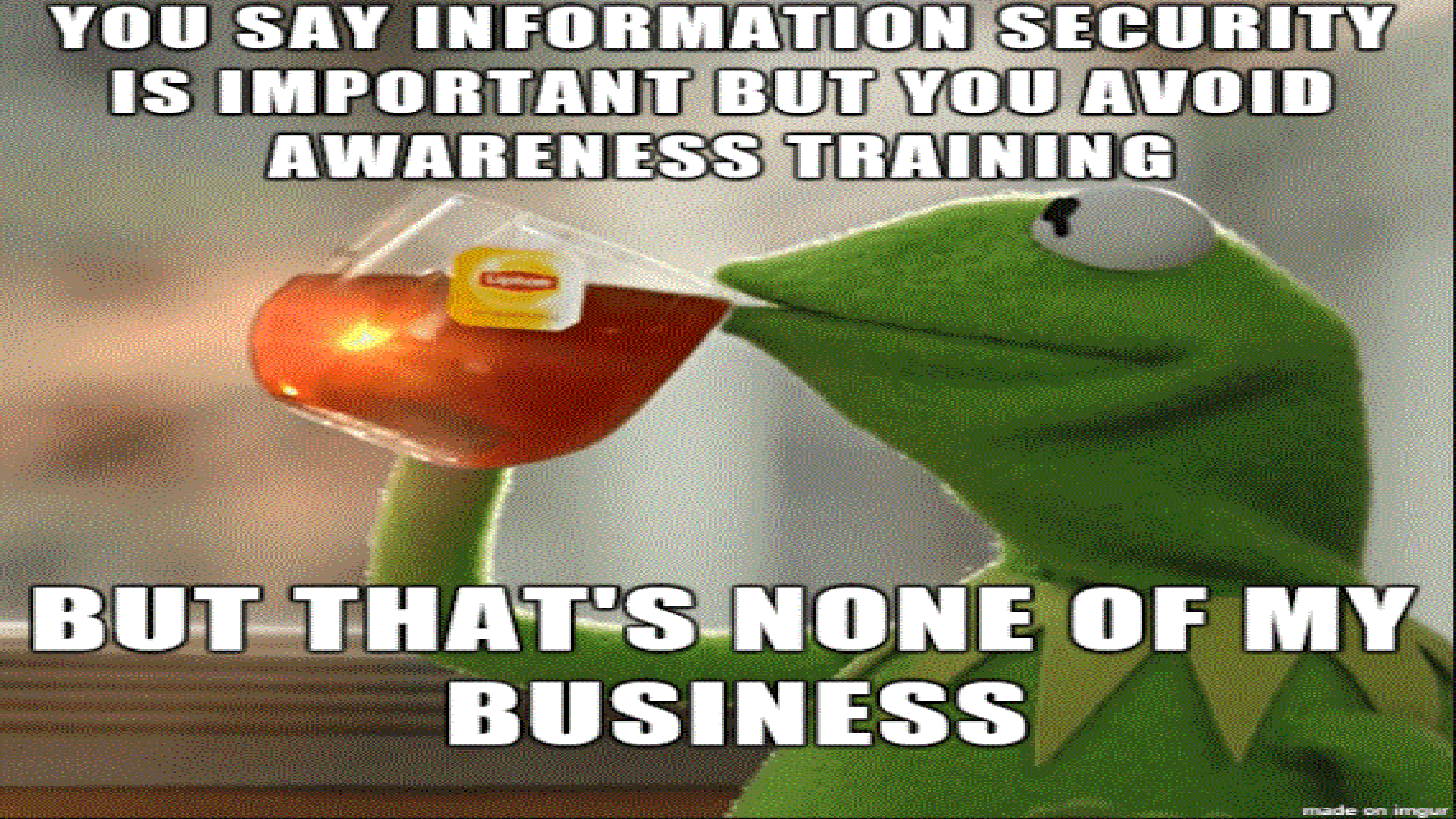
Secure Bank Accounts

- 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

Tips To Secure Your Devices From Cyber Attacks

SECUREB4
We Strengthen Your Security

- Use strong passwords
- Enable two-factor authentication
- Keep your software up-to-date
- Install a reputable security suite
- Use a VPN (Virtual Private Network)
- Be aware of phishing scams
- Avoid public Wi-Fi
- Use a firewall
- Back up your data
- Educate yourself about latest cyber threats


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

FRANK'S®
RedHot®
RedHot
I put that on everything™

Cybersecurity myths

- My organization is too small or to be a target
- My data (or the data I have access to) isn't valuable
- Attacks are always technically complex
- New software and devices are secure out-of-the-box
- Cybersecurity requires a huge financial investment
- Cyber breaches are covered by insurance
- **Security is an IT issue**

My Personal Tech Stack

- Email: Proton mail
- VPN: Proton VPN
- Password Manager: 1Password
- File sharing: Proton / MS OneDrive
- MFA Autheticator: Authy / MS Authenticator
- A/V: MS Defender
- Firewall: MS Firewall
- Brower: Firefox, Brave, Safari
- Search Engine: DuckDuckGo, Brave, StartPage
- Encryption: BitLocker

For more information

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

intrust IT

Additional Resources

- www.microsoft.com/security
- security.microsoft.com/securescore
- securityscorecard.com
- 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.idtheftcenter.org/facts.shtml
- www.cisa.gov
- www.fbi.gov
- www.ic3.gov/default.aspx
- www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
- enterprise.verizon.com/resources/reports/dbir/
- www.sans.org
- www.us-cert.gov/ncas/current-activity/2019/11/06/cisa-launches-cyber-essentials-small-businesses-and-small-sltt
- 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.techradar.com
- foundation.mozilla.org/en/privacynotincluded
- www.plunkfoundation.org

intrust IT

Questions?

“Cybersecurity is national security”

- NSA Director General Paul Nakasone

Thank You!

Dave Hatter, CISSP, CISA, CISM, CCSP, CSSLP, PMP, ITIL

linkedin.com/in/davehatter
twitter.com/davehatter

Get our checklist:
https://www.intrust-it.com/cyber-security/cyber-essentials-checklist

ASK ABOUT OUR NO-COST, NO-OBLIGATION IT ASSESSMENT

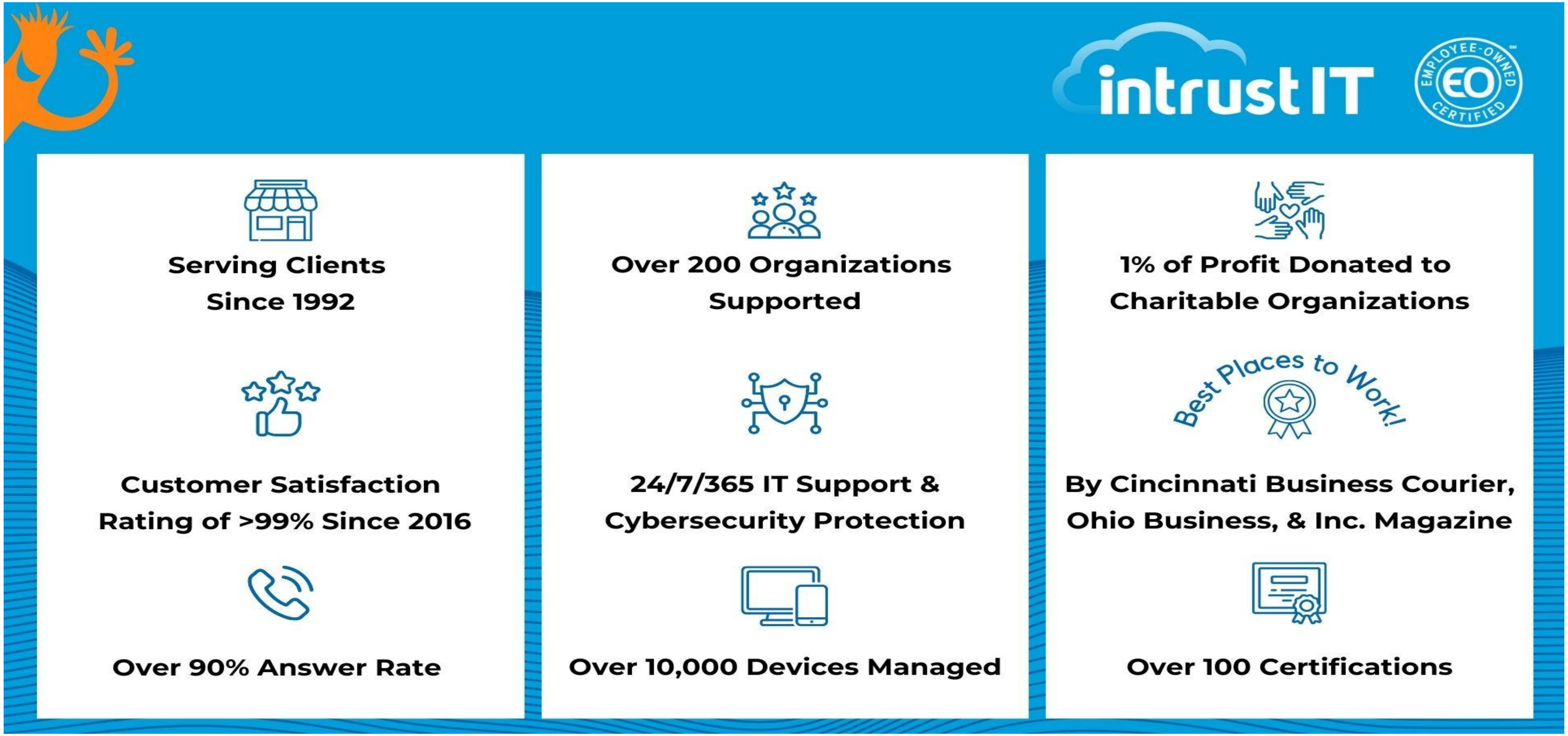
- **Catch Tech Friday live on 55KRC at 6:30 AM every Friday on 550 AM or http://55krc.iheart.com**
- **Catch Cyber Monday live on WTVG at 6:30 AM and Tech Support at 9:00 AM every Monday on 13 ABC or https://www.13abc.com/**

intrust IT

WE ARE NO LONGER
SECURING COMPUTERS

WE ARE SECURING SOCIETY.

Intrust At a Glance



intrust IT

EMPLOYEE-OWNED EO CERTIFIED

Serving Clients Since 1992

Over 200 Organizations Supported

1% of Profit Donated to Charitable Organizations

Customer Satisfaction Rating of >99% Since 2016

24/7/365 IT Support & Cybersecurity Protection

Best Places to Work! By Cincinnati Business Courier, Ohio Business, & Inc. Magazine

Over 90% Answer Rate

Over 10,000 Devices Managed

Over 100 Certifications

intrust IT