



Cybersecurity and the Small Business Sector


A grayscale background image showing a person from the chest up, wearing a light-colored sweater. They are looking down at a small object, likely a smartphone, held in their hands. The background is blurred, suggesting an indoor setting with a table and other objects.


What every employee must know about the
vulnerabilities of working outside the company network,
and your role in protecting the company.

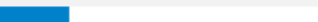
Why Businesses are Prime Targets


- ❑ On average 10% of their annual budget is spent on IT and support.
- ❑ Many lack cybersecurity practices, paired with aging equipment and unpatched devices.
- ❑ Some don't believe it will happen to them
- ❑ Others believe their data is 'not-valuable enough.'
- ❑ Most are behind the in educating employees

Who are the victims?

24% 
of breaches affected healthcare organizations

15% 
of breaches involved accommodation and food services

14% 
were breaches of public sector entities

58% 
of victims are categorized as small businesses

Source: Verizon 2018 DBIR Report

FBI Reported Losses Due to BEC/EAC Since October 2015

FBI BEC update:
\$26.2B

FBI BEC update:
\$12.5B

FBI BEC update:
\$5.3B

FBI BEC update:
\$1.2B

FBI BEC update:
\$3.1B

2015

2016

2017

2018

2019

Chart adjusted based on FBI ic3 reports over time

2020 \$10.2 Billion in Victim Losses Reported

Source: https://pdf.ic3.gov/2020_IC3Report.pdf

Corporate Data Breach \$53,398,278	Personal Data Breach \$120,102,521	Credit Card Fraud \$111,491,163
Business Email Account \$1,776,549,688	Identity Theft \$160,305,789	Investment Fraud \$222,186,195

The Internet Crime Complaint Center (IC3) analyzes complaints submitted by victims of internet crimes.

Threat Vectors

(How The Bad Guys Get In)



Phishing, Web & Ransomware



Compromised Credentials



Weak Passwords



Trust Relationships & Propagation



Poor Encryption



Unpatched Vulnerabilities



Misconfigurations



Malicious Insiders



Zero Day & Unknown Methods

A grayscale photograph of a person wearing a grey sweater, looking down at a device held in their hand. The image is split horizontally by a red banner containing text.

“How likely am I to be hacked?”



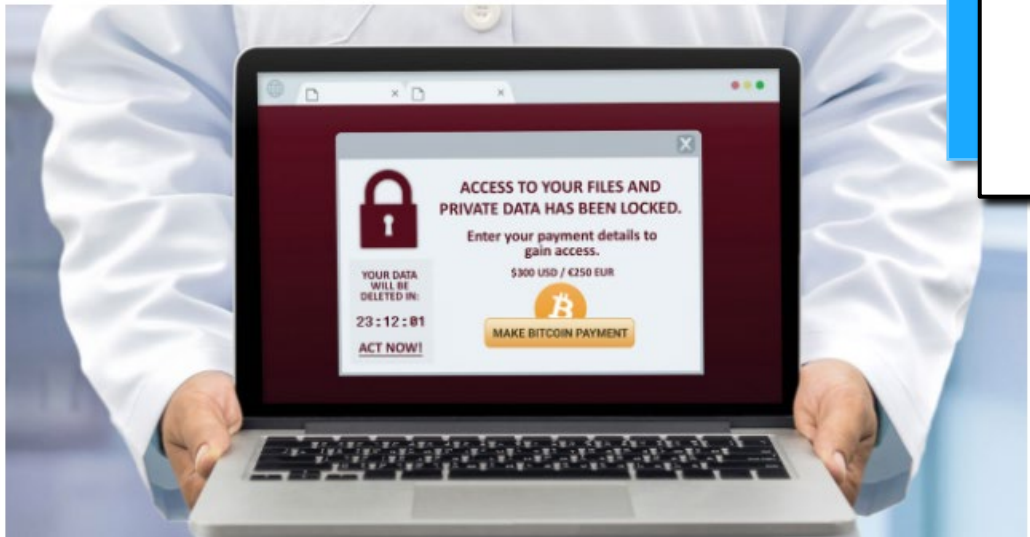
Help Net Security
April 21, 2020

Share



46% of SMBs have been targeted by ransomware, 73% have paid the ransom

Ransomware attacks are not at all unusual in the SMB community, as 46% of these businesses have been victims. And 73% of those SMBs that have been targets of ransomware attacks actually have paid a ransom, Infrastyle reveals.



MARKETS

BUSINESS

INVESTING

TECH

POLITICS

CNBC TV

SMALL BUSINESS PLAYBOOK

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

PUBLISHED SUN, OCT 13 2019 10:30 AM EDT

Source: <https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html>



A New Ransomware Attack Occurs Every

14 Seconds

(By 2021, it will be every 11 seconds)

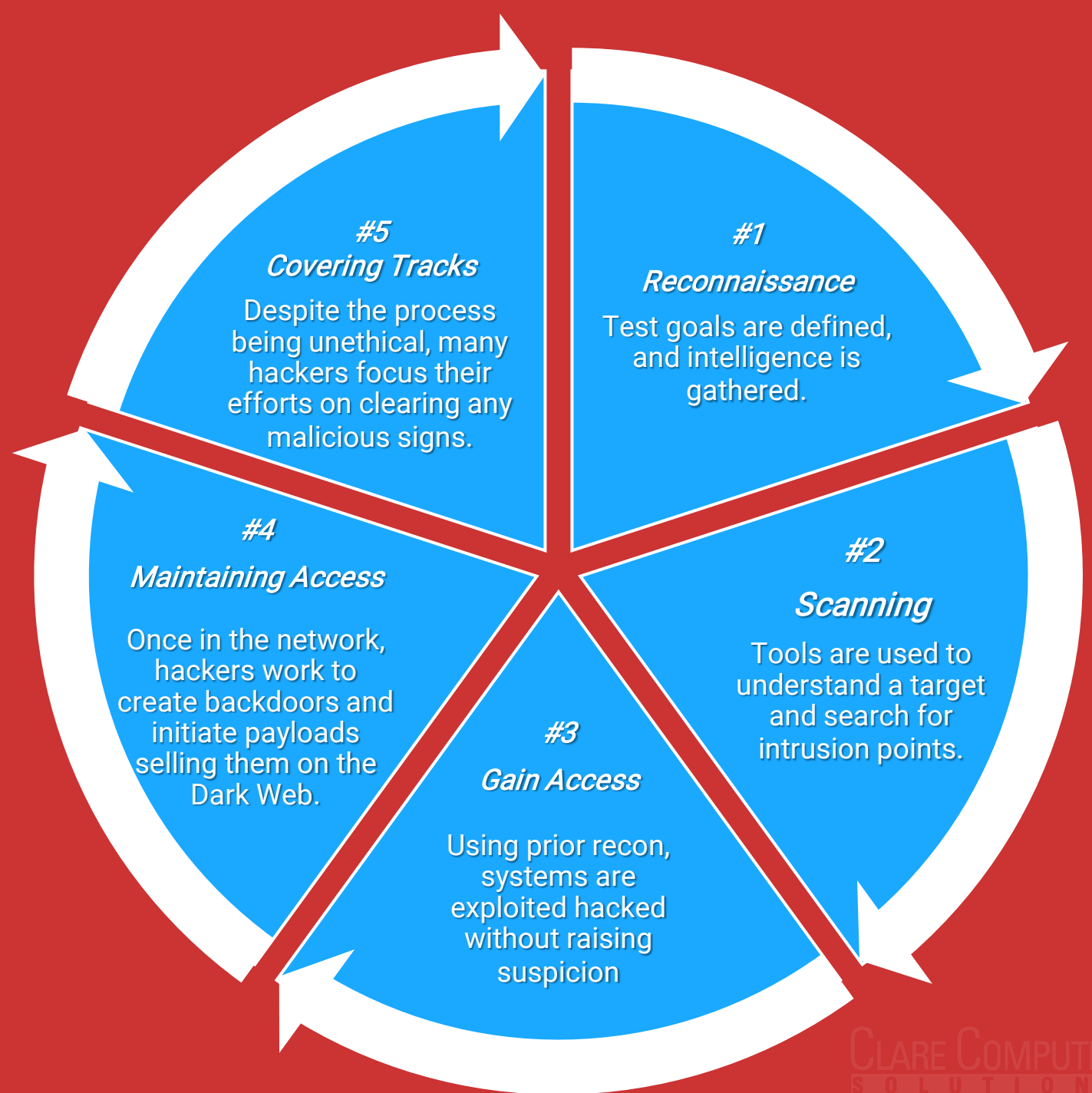


“What is the workflow of a hacker?”

The Workflow of a Hacker

- Many of the tools used are free online or for download
- In many cases these steps can be automated for quick attack
- On average hackers stay in a network for over 191 dates.
- 38% of attacks are missed by Anti-Virus

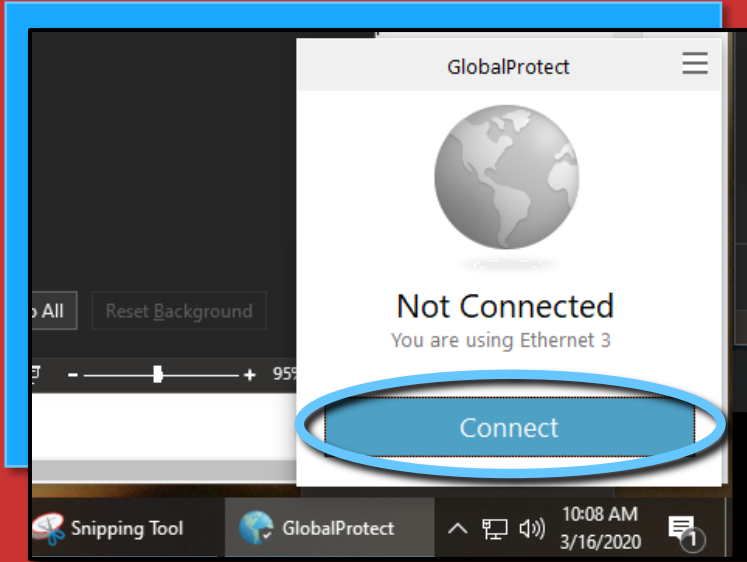
Source: SentinelOne



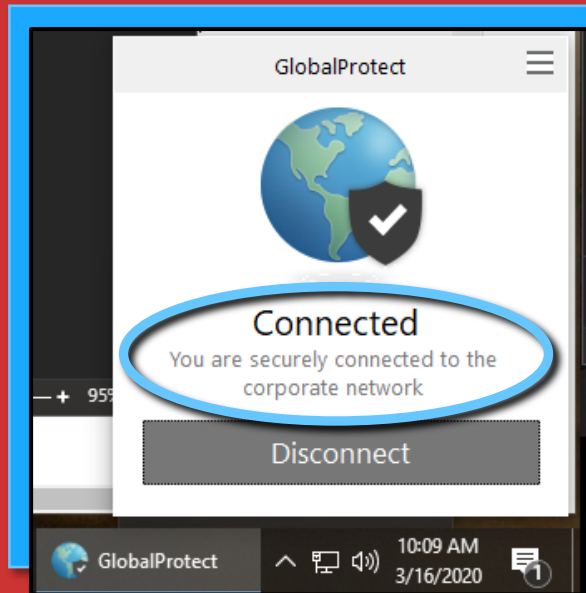
A grayscale background image showing a person from the chest up, wearing a light-colored sweater. They are looking down at a small object, likely a smartphone, which they are holding with their right hand. The background is blurred, suggesting an indoor setting with a table and other objects.

“What are some of the ways you can avoid external network or company threats?”

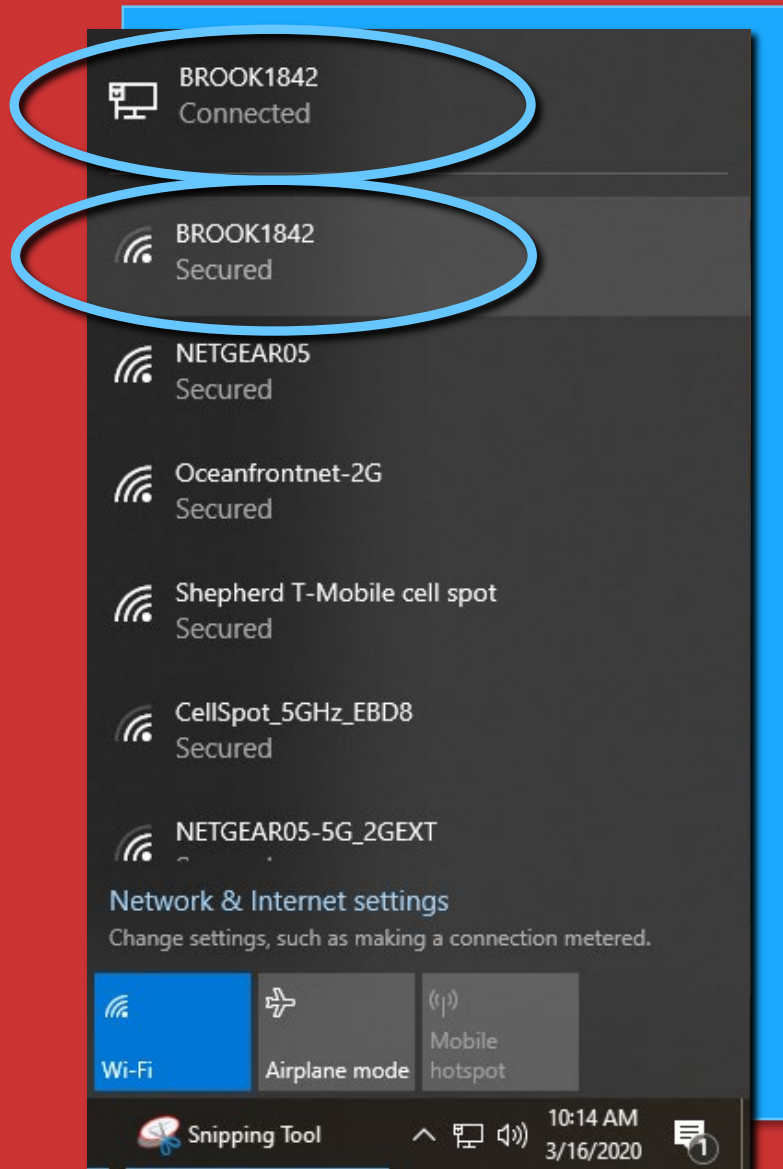
Connecting a Company VPN



1. What is a VPN? It's a "Virtual Private Connection." Essentially, it creates a private tunnel through the Internet for your computer to access company digital resources.
2. If Your Company Provides a VPN Connection, Obtain the Instructions Before You Leave the Office with the Equipment You'll Need
3. Test the Setup and Connection Before You Start Working on Company Data from the Home Computer
4. Shutting Down or Restarting Your Computer will Disconnect the VPN. Your IT Person May Have Specific Instructions on the Disconnect Procedure for You.



Turn Off Options for Automatic Wi-Fi Connection



1. Look at each Wi-Fi connection you have used in the past. You might have selected a different, less secure signal (i.e. the Starbucks across the street) and checked "Connect Automatically." That signal could be taking priority over a more secure signal you should be using.
2. If you are connected to the wrong signal, click on it and select "Forget this Network." That will force your computer to sign into that network manually next time.
3. Connect to the most secure network you can, at all times. We recommend you NEVER connect to a network that is not password protected, even if you're using a VPN.

Uninstall Google Chrome Extensions

500 Malicious Chrome Extensions Impact Millions of Users



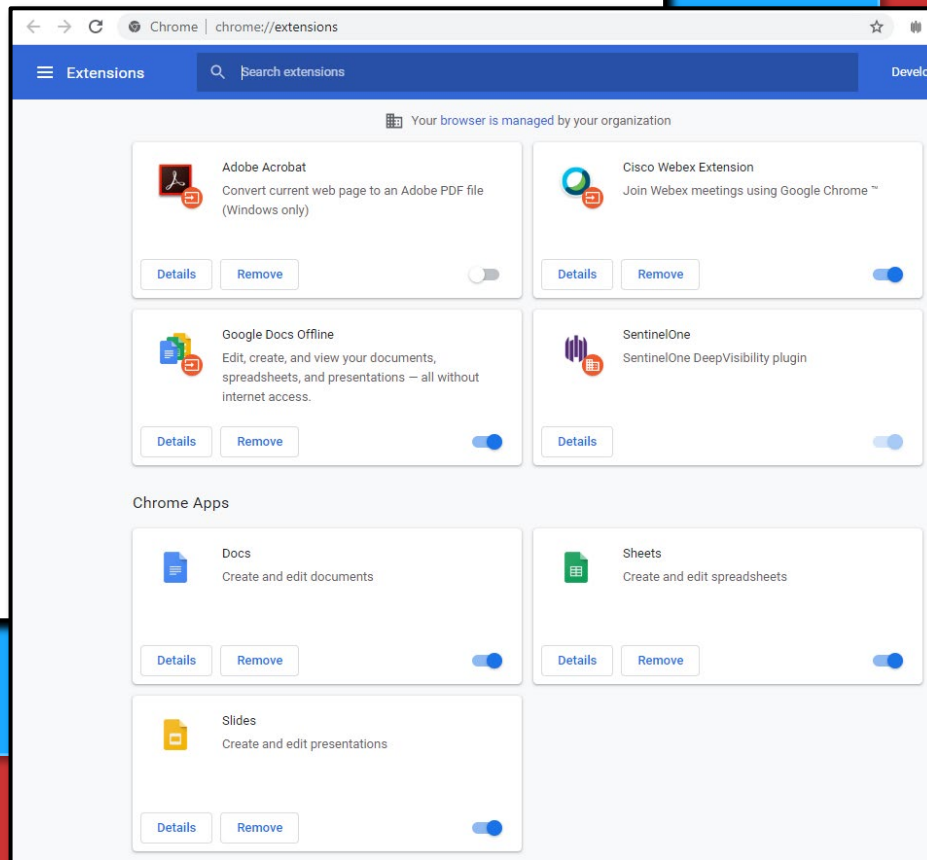
Author:
Lindsey O'Donnell

February 14, 2020
/ 3:50 pm

3 minute read

Write a comment

Share this article:



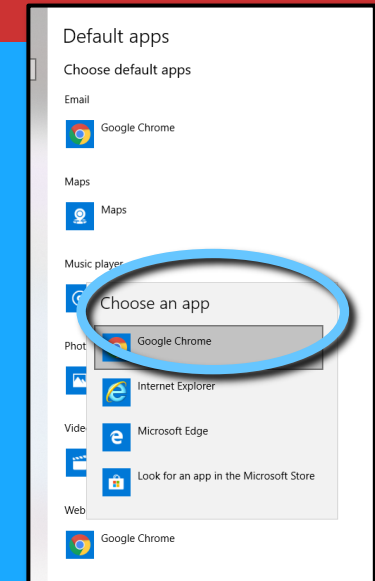
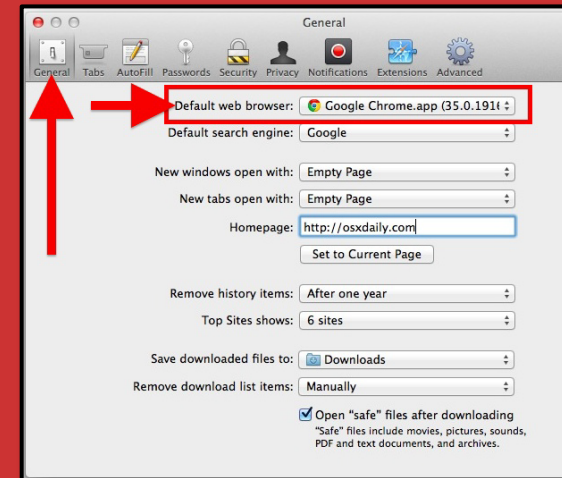
1. We get it, if you use it, you might need it. But if you're not using an extension, it's good to uninstall it. Many of the extensions created years ago and posted in the Google Chrome Extension library, had been sold to malicious actors, or are no longer supported.

Use Google Chrome/Firefox to Browse

PC – click the Win key and type “Default” then select “Default Apps” from the top of the Start Menu. Scroll down to Web Browser and Select Chrome or Firefox.

1. Default browsers (whether it's Internet Explorer for the PC, or Safari for the Mac) are not as secure as Google Chrome or Firefox.
2. After you install an alternate browser, change the default browser selection:
















Mac – In Preferences, go to the General tab and Use the Drop-Down menu to select Chrome or Firefox.




15 Ways To Protect Your Business From A Cyber Attack!



15 Ways To Protect Your Business From A Cyber Attack!

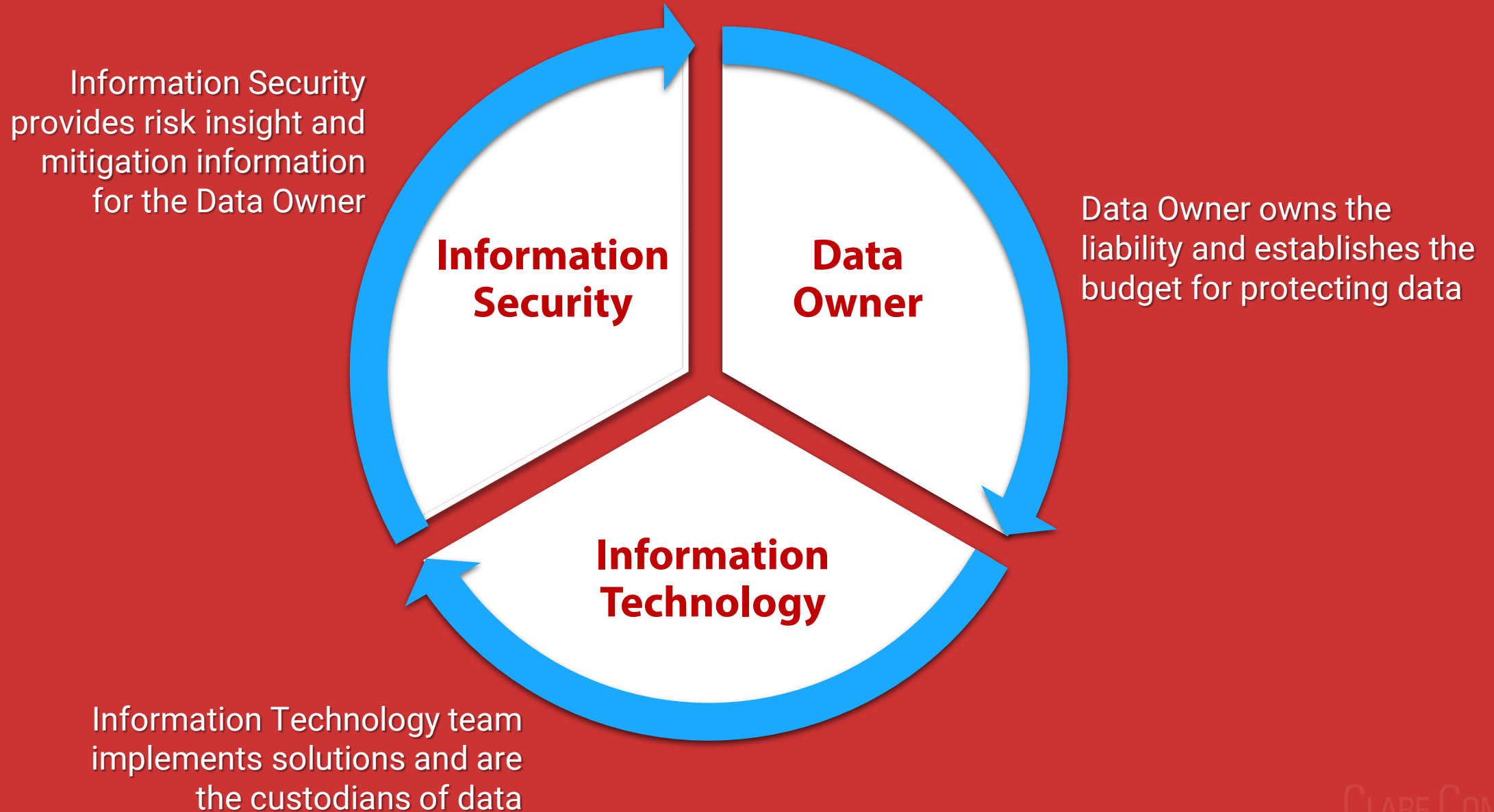
 Security Assessment It's important to establish a baseline and close existing vulnerabilities. When was your last assessment? Date: _____	 Spam Email Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.	 Passwords Apply security policies on your network. Examples: Deny or limit Use file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.
 Security Awareness Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.	 Did you know? 1 in 5 Small businesses will suffer a cyber breach this year. 81% Of all breaches happen to small and medium sized businesses. 97% Of breaches could have been prevented with today's technology.	 Advanced Endpoint Detection & Response Protect your computers adsafe from malware, viruses, and cyber attacks with advanced endpoint security. Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script-based threats and can even roll back a ransomware attack.
 Multi-Factor Authentication Utilize Multi-Factor Authentication whenever you can including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your account is protected.	 Computer Updates Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.	 Dark Web Research Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.
 SIEM/Log Management (Security Incident & Event Management) Uses big data engines to review all event and security logs from all covered devices and protect against advanced threats and meet compliance requirements.	 Web Gateway Security Internet security is a race against time. Cloud based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds - before they reach the user.	 Mobile Device Security Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes the gap.
 Firewall Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!	 Encryption Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.	 Backup Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.

 **Cyber Insurance** If all else fails, protect your income and business with cyber damage and recovery insurance.



**“What responsibilities do employees really have,
when it comes to cyber security?”**

Data Responsibility

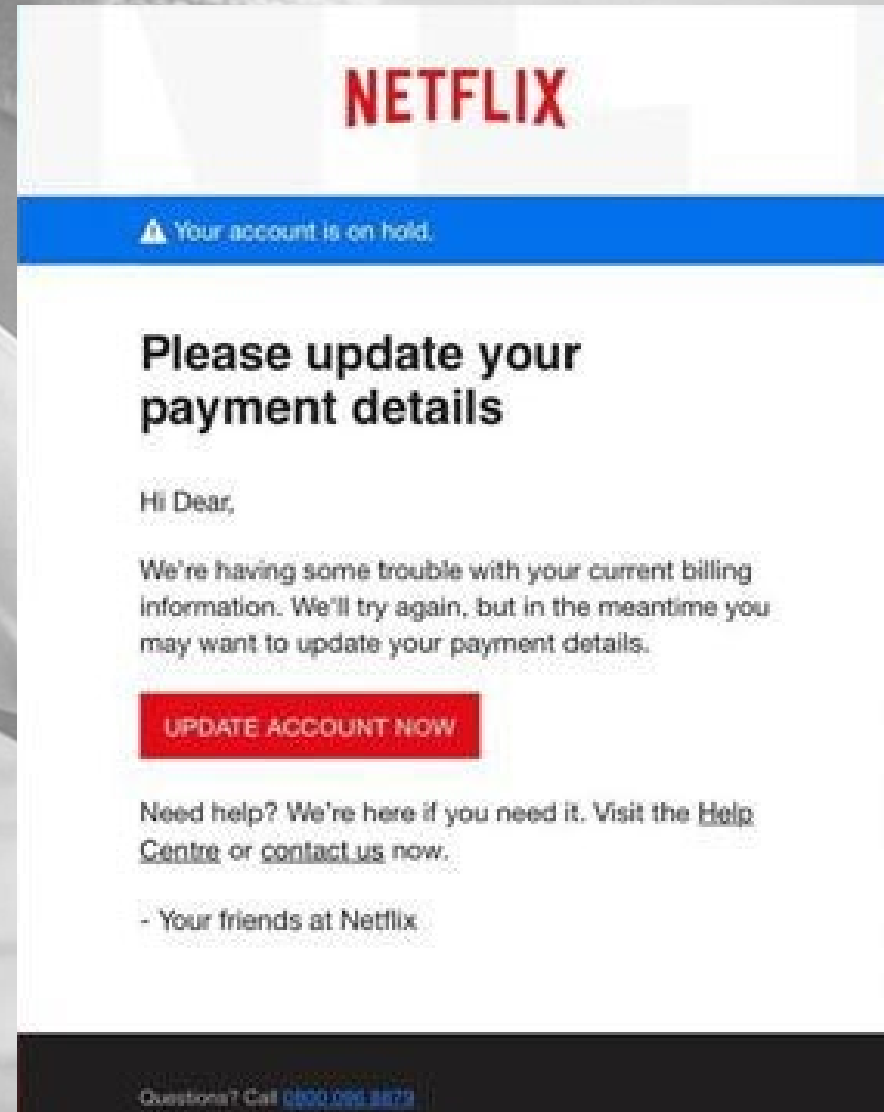


Employees Are Our 1st Line of Defense

- *2020 Average data breach costs 3.92 Million*
- *Hackers attack every 39 seconds*
- *Averaging 2,244 Attacks Per Day*

Arm employees with the knowledge to:

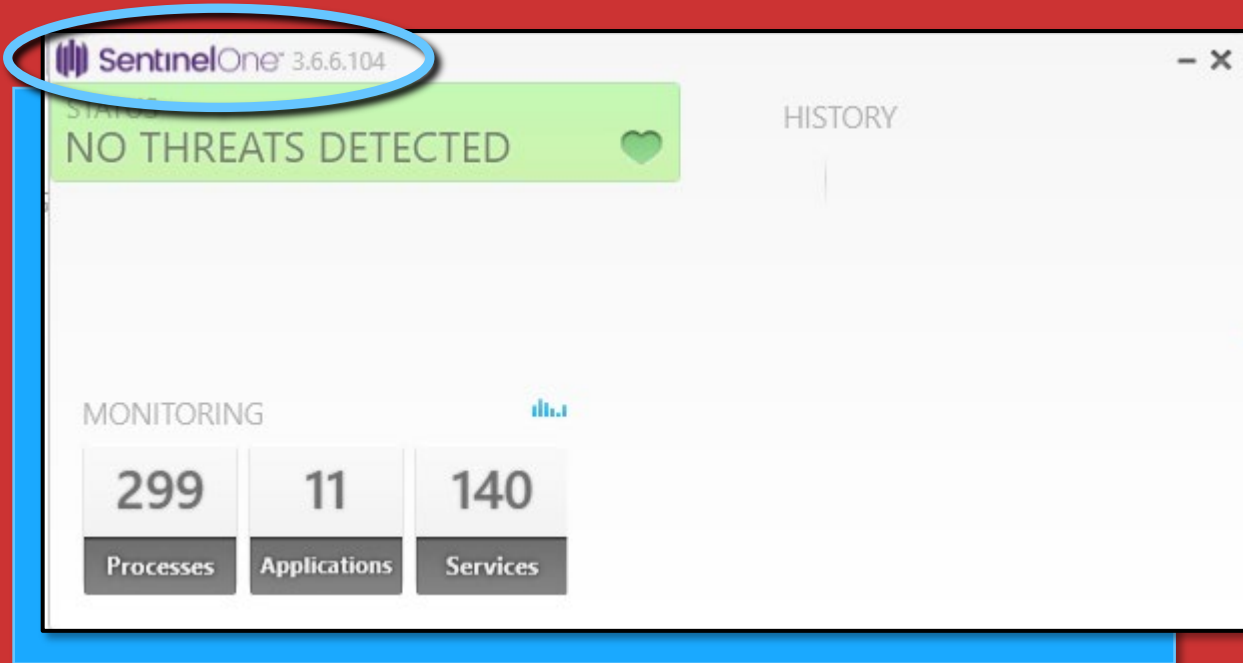
- Spot Phishing Scams
- Malicious Links
- Remote Desktop Requests
- Suspicious Attachments



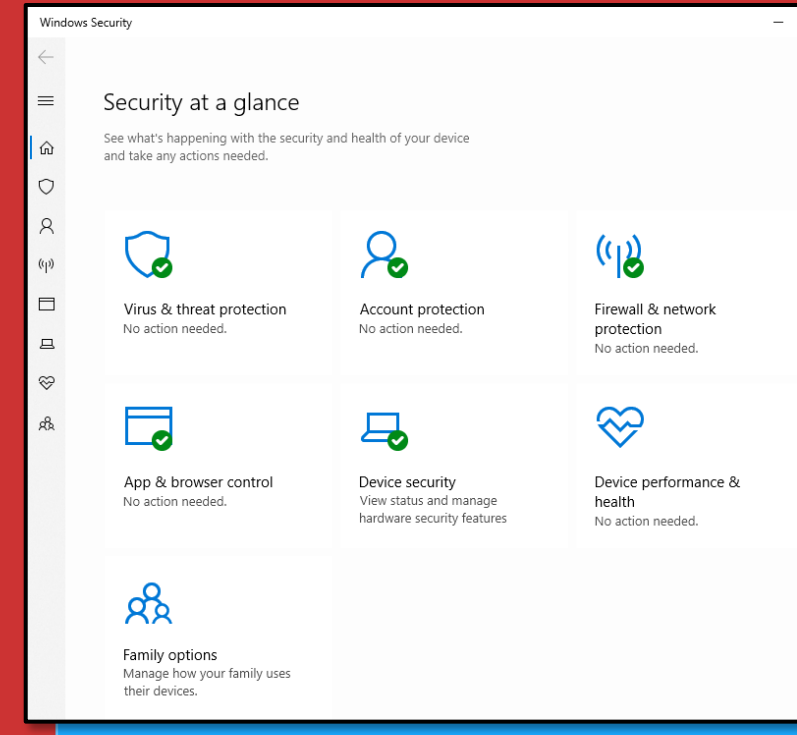


“Endpoint Detection & Response Vs. Anti-Virus How Does It Work?”

Update Anti-Virus to Anti-Malware



1. We recommend you have a paid, subscription-based AV program, make sure it shows the most current version running. It may have a “Check for Updates” button to click, or it should say “Your program is up-to-date.”



1. If you have a PC, go to the Windows Security Screen by hitting the Win button on the keyboard and typing “windows security” – it will be at the top of the start menu.
2. Any items not updated properly will have a red mark indicating it needs attention.



“How can employees or business owners discover if their data was leaked? Can something be done?”

Cybercrime on the Dark Web

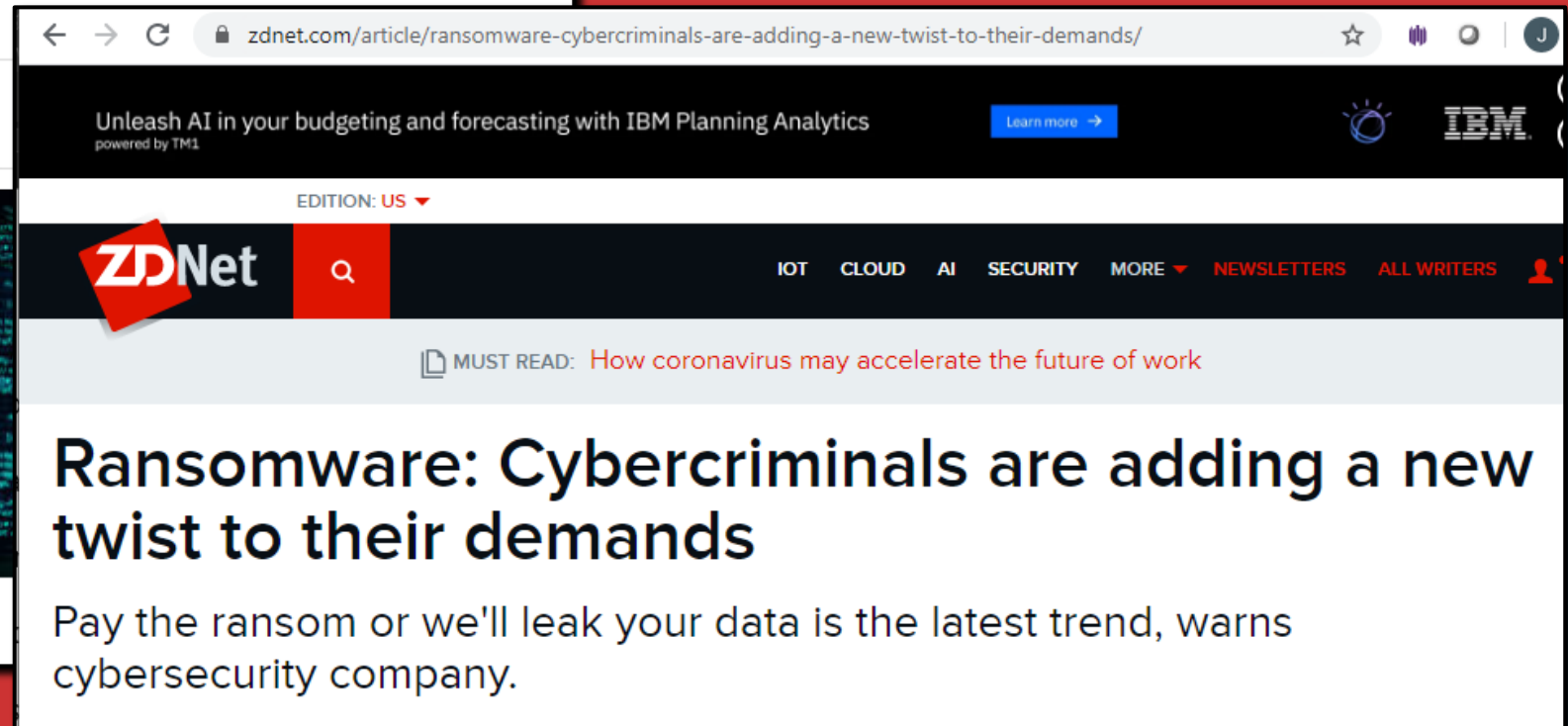
Ransomware Attacks Costs Nearly Triple in 2019 to over \$36K Per Attack

Stu Sjouwerman

[Tweet](#) [Share](#) [Like 31](#) [Share](#)

The latest data from [ransomware](#) recovery vendor, Coveware, outlines the current state of the cost, duration, and recovery rate of ransomware attacks today.

Many organizations still think ransomware is merely a nuisance, impacting only a few machines and requiring only restoring backups to address. But the [Coveware Q2 Ransomware Marketplace Report](#) tells a different story.



The screenshot shows a web browser displaying a ZDNet article. The address bar shows the URL: zdnet.com/article/ransomware-cybercriminals-are-adding-a-new-twist-to-their-demands/. The page features a dark header with the ZDNet logo, a search bar, and navigation links for IOT, CLOUD, AI, SECURITY, MORE, NEWSLETTERS, and ALL WRITERS. A banner at the top promotes IBM Planning Analytics. Below the header, a 'MUST READ' section highlights the article. The main headline reads 'Ransomware: Cybercriminals are adding a new twist to their demands', followed by a sub-headline: 'Pay the ransom or we'll leak your data is the latest trend, warns cybersecurity company.'

Unleash AI in your budgeting and forecasting with IBM Planning Analytics powered by TM1 [Learn more](#)

EDITION: US

ZDNet [Q](#)

IOT CLOUD AI SECURITY MORE NEWSLETTERS ALL WRITERS

MUST READ: [How coronavirus may accelerate the future of work](#)

Ransomware: Cybercriminals are adding a new twist to their demands

Pay the ransom or we'll leak your data is the latest trend, warns cybersecurity company.

What is a Dark Web Report and Why Does It Matter?

Discovery if your business has been compromised. See if hackers are selling your important data!


Security Evaluation for Site: Bluth Company




The dark web is a massive and widely used marketplace by cyber criminals



Malicious actors use stolen email credentials to impersonate the owner to commit theft or other fraud



The stolen records including identity and credit card information are often sold on the dark web



DARK WEB FACTS

RISKS DETECTED FOR YOU

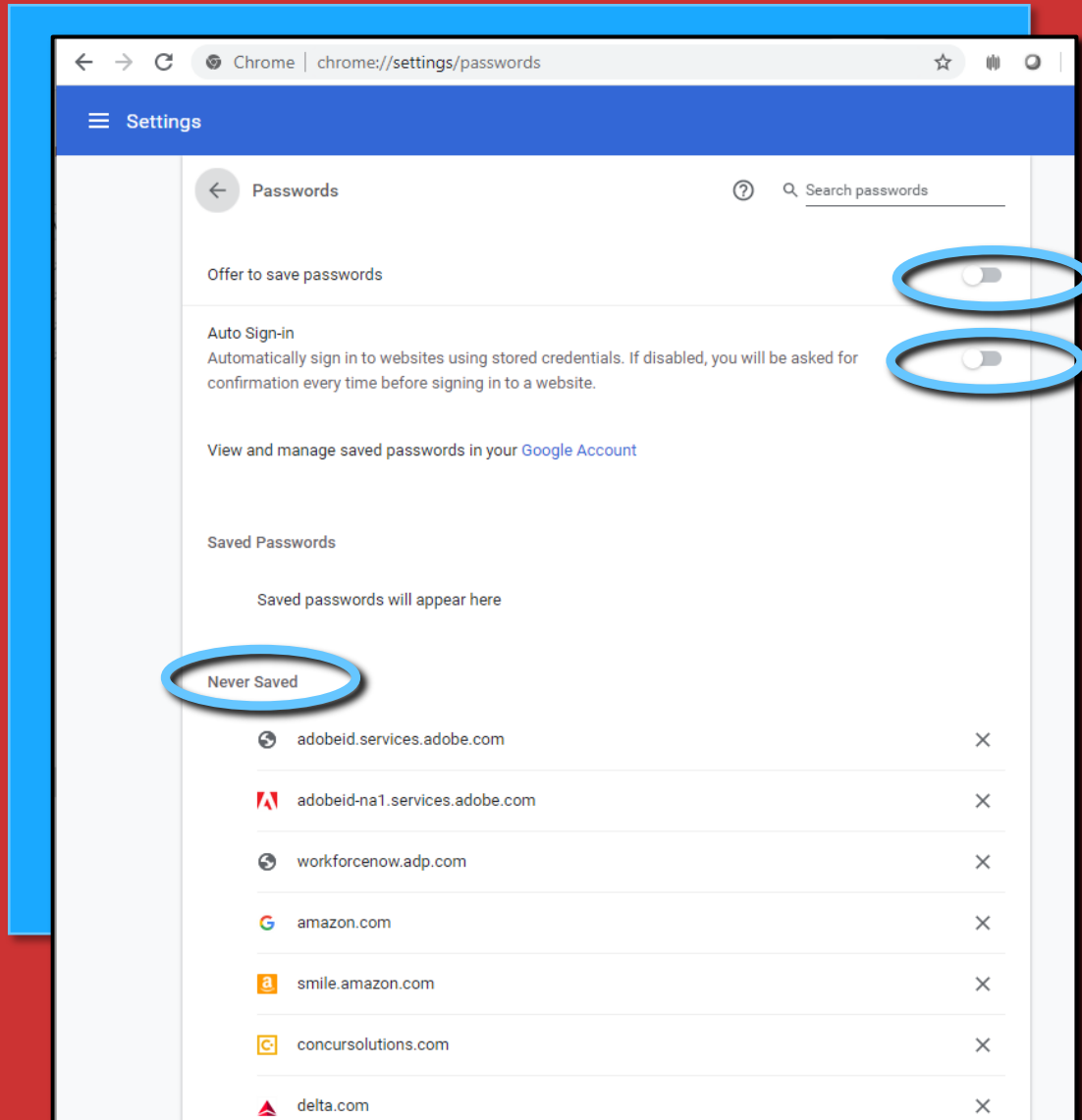
03

UNIQUE EMAIL IDS FOUND

Some email IDs may have multiple breaches

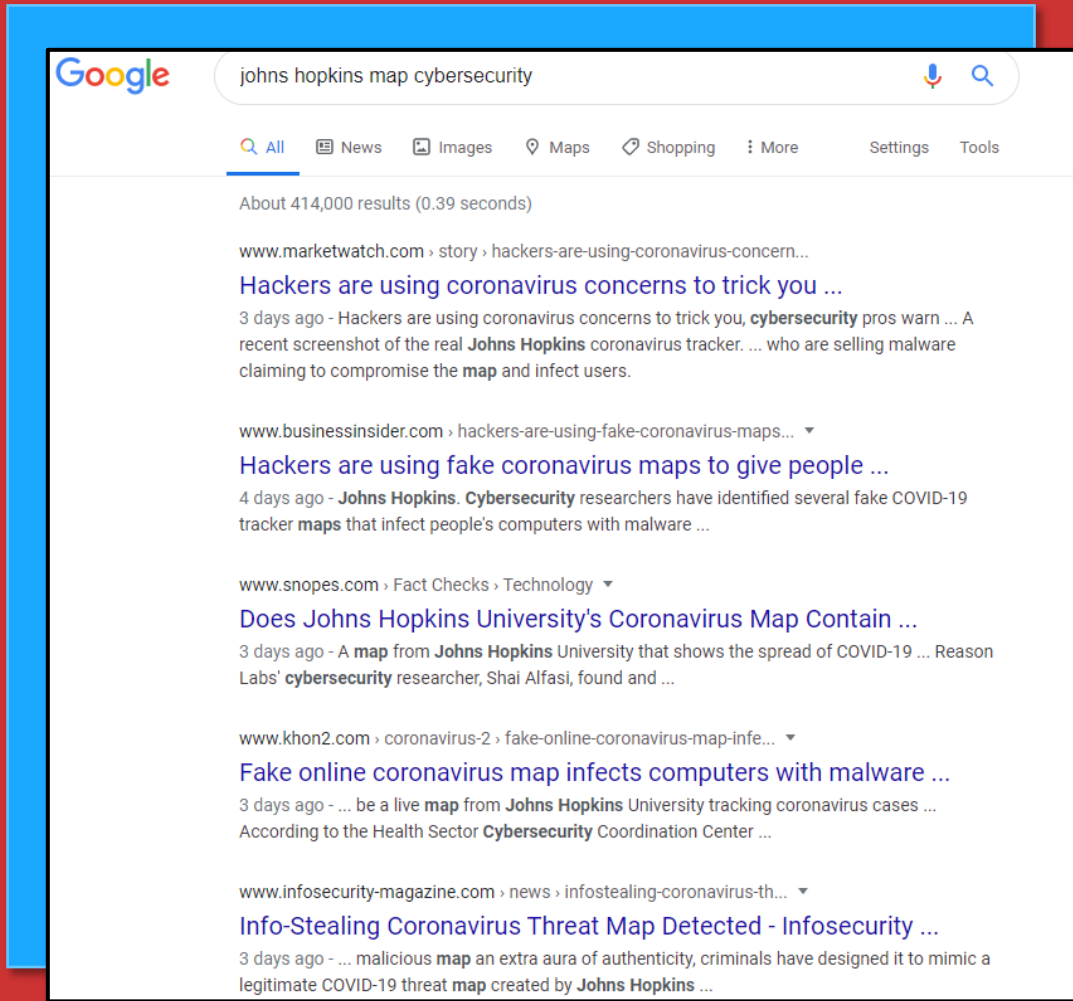
Email ID	Password	Publish Date	Breach Source
admin@example.org	r3v*****	Feb 05, 2019	Not Disclosed
admin@example.org	r3v*****	Jan 28, 2019	Not Disclosed
admin@example.org	r3v*****	Jan 24, 2019	Not Disclosed
admin@example.org	orp*****	Dec 19, 2018	Not Disclosed
admin@example.org	Encrypted	Dec 12, 2018	Not Disclosed
admin@example.org	Encrypted	Feb 17, 2018	disqus.com
admin@example.org	Encrypted	Feb 17, 2018	kickstarter.com
admin@example.org	r3v*****	Dec 21, 2017	Not Disclosed
admin@example.org	orp*****	Mar 14, 2017	mobango.com
admin@example.org	r3v*****	Jan 30, 2017	crackingforum.com
jake@example.org	123*****	Feb 05, 2019	Not Disclosed
jake@example.org	123*****	Jan 28, 2019	Not Disclosed
jake@example.org	123*****	Dec 19, 2018	Not Disclosed
jake@example.org	123*****	Dec 21, 2017	Not Disclosed

Got Passwords?



1. Use a password manager to save them. Some examples: Password Boss, Passportal, LastPass, Dashlane, 1Password, KeeperMSP, etc.
2. Never allow your browser to save passwords or to auto-login.
3. Never save your passwords in a Word or Excel document on your computer. If you MUST do so, do not name it "Passwords," name it something like "Mom's Chicken Soup Recipe" and do not use the word "password" anywhere in the document itself (it will show up in a search). And password-protect that document, so if someone else tries to open it, they can't do so without the password.

Think Twice



1. You're in an unfamiliar environment for working on company data. Don't take anything for granted.
2. You might be tempted to mix in personal "computing" that you wouldn't normally do during work. Is that music application, video link that your spouse emailed to you, etc. really important to open now?
3. Scouring the news for what's happening world-wide and right in your own neighborhood might be important. But be careful what you click on! Take the time to do a safe web search.
4. Hackers know most people are not working behind their office firewall. They are actively seeking to exploit users and steal the company assets.



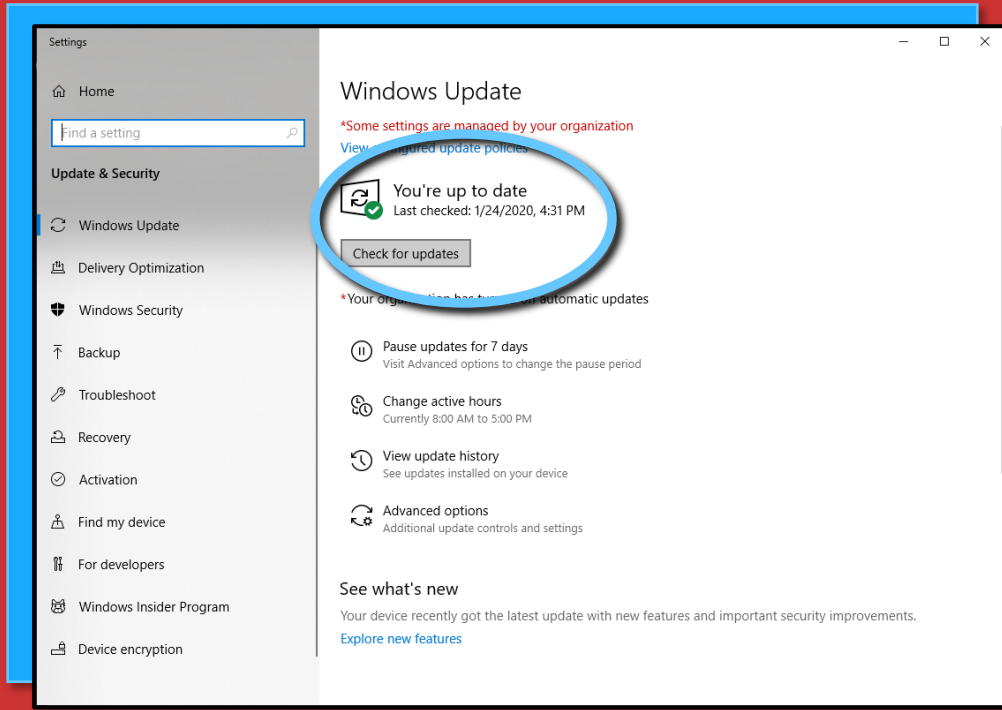
“What are some cost-effective solutions we can focus on internally?”

Lock Your Computer When Not in Use

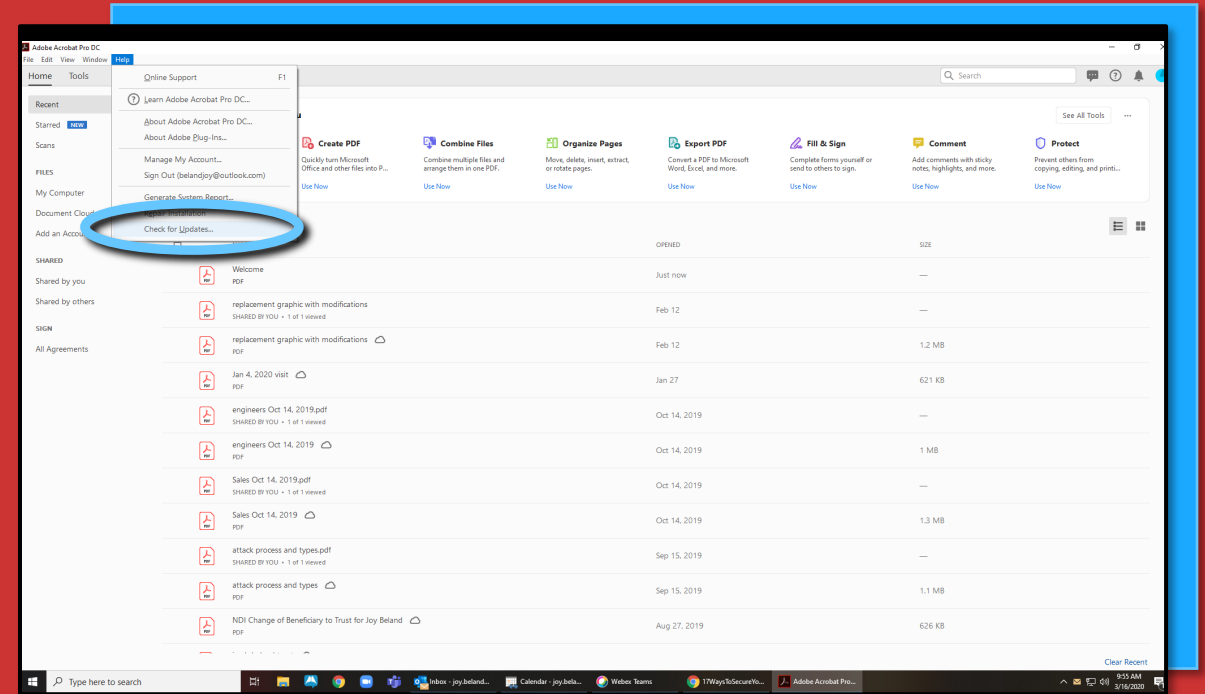


1. Especially Important if You Work Remotely in a Public Area, Like a Starbucks
2. Important if You Have Children or Spouses Around
3. What is Private at Work Should be Treated as Private Remotely

Install Updates

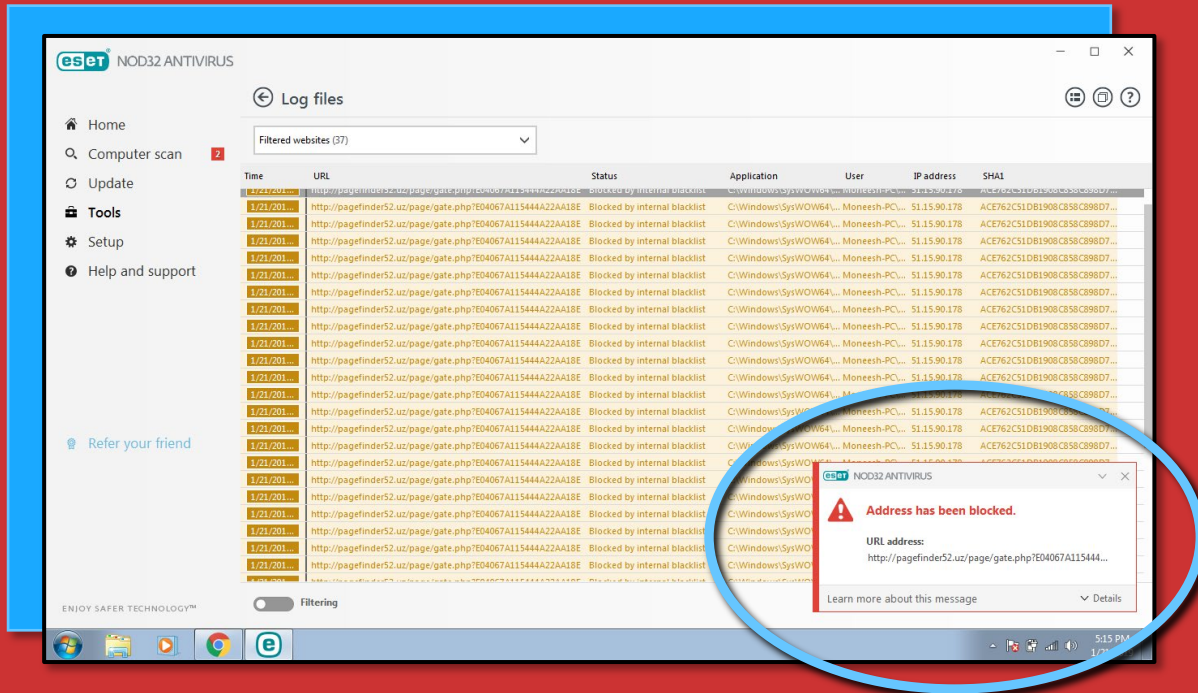


1. Windows Updates – hit the Win key and type “update” and you’ll see the “Check for Updates” option at the top of the Start Menu. Select that. You’ll see if your system is up to date, or where to initiate the Check for Updates here.
2. If you need updates, close all programs before proceeding. You may need to restart your computer for the updates to take effect.



1. Software Updates – Most commonly Adobe, Microsoft Office (Word, Outlook, etc).
2. Most programs allow you to open and select “check for updates” from the Help menu.
3. Once the update initializes, close the program so the installation can complete. You may need to restart your computer when the update is done.

Use a DNS Filter

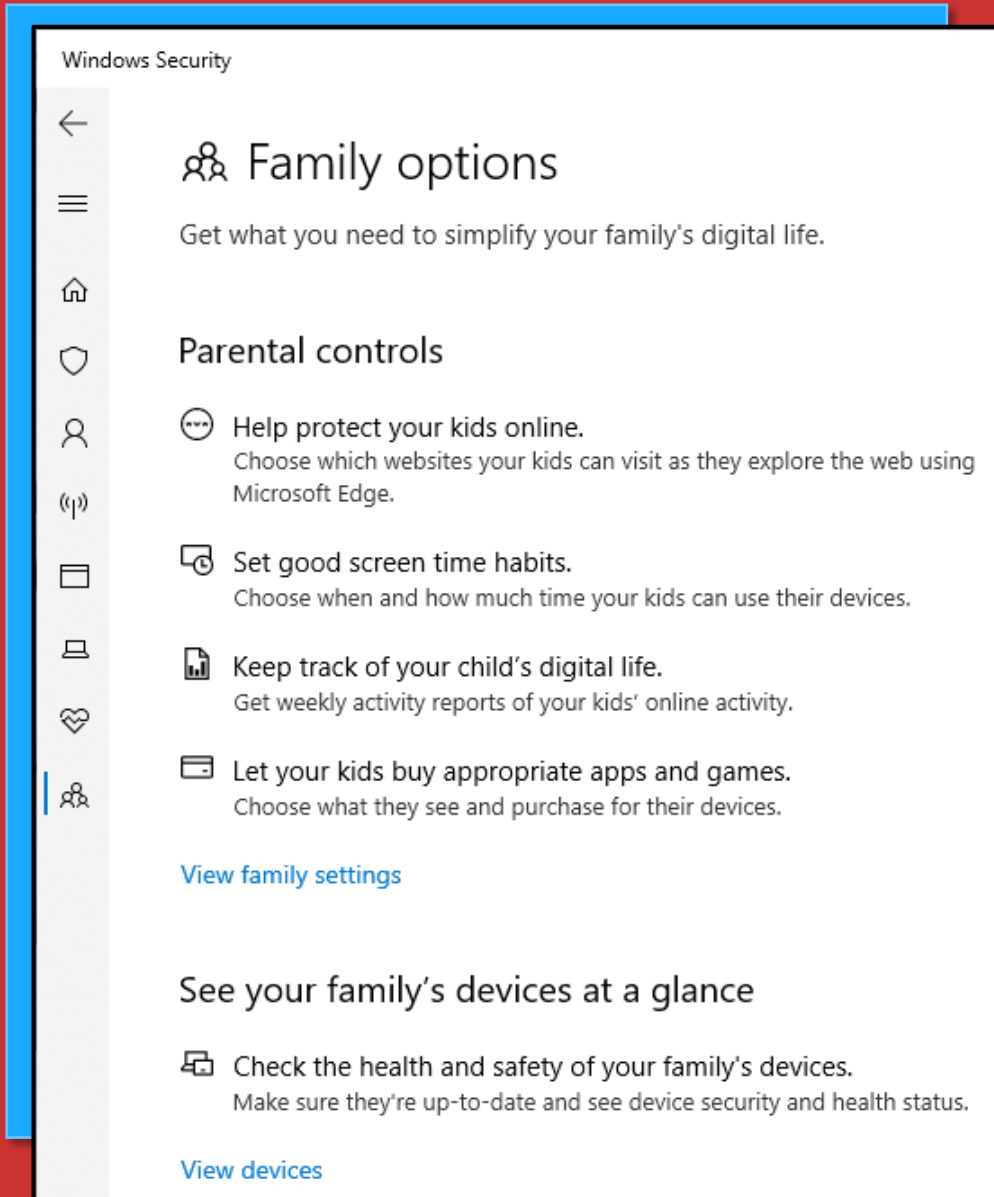


1. What is DNS? It's essentially a phone book of all known domains and matching "addresses" for the internet. It contains every website domain, whether it is malicious or reputable.
2. There are security solutions that subscribe to a list of known bad domains. They are called DNS filters. When you try to click on a website URL or do an internet search, a DNS filter will block a malicious website in most cases.
3. Check with your IT provider to see if they have something you can install on your home computer to serve this purpose.



“How ‘at-risk’ are we with our employees using personal devices while working?”

Create a Separate User Profile

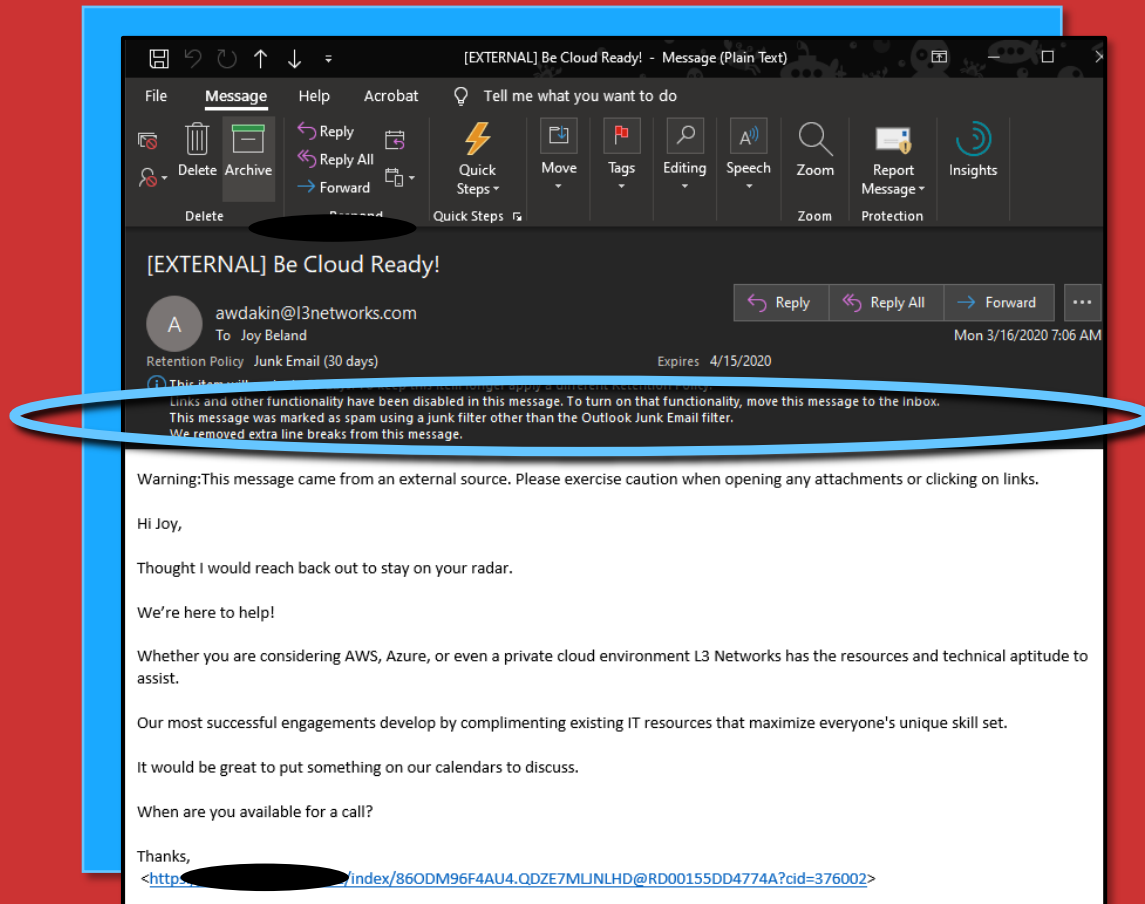


1. It's preferred to dedicate one computer to working remotely (not shared with spouse or children).
2. If you need to share computers, be sure to set up separate User Profiles, and enable Parental Controls on the children's User Profiles.
3. Remember this rule of thumb – if it's free, it probably has spyware on it. If you don't need it, don't install it.

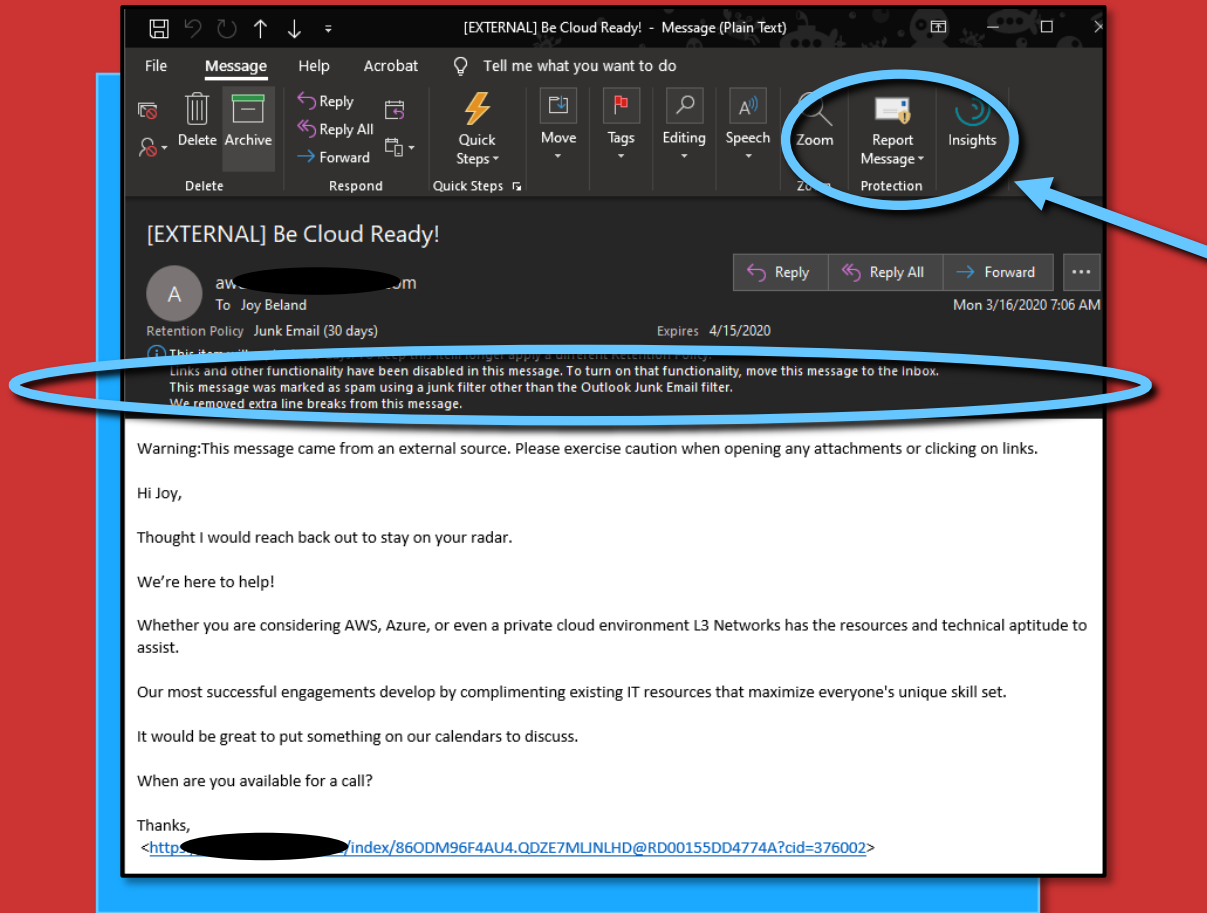
Don't Be Click Happy

Think About What You Might Not Have on Your Home Computer, That is Probably on Your Office Network:

- ☐ Office 365 Advanced Threat Protection which Serves as a Primary Filter for Infected or Malicious E-mails
- ☐ E-mail Filters Via (Vendor) for Infected Attachments and Known Malicious Links
- ☐ DNS Filtering for All Requests Sent From Your Computer to the Internet, Blocking Known Malicious Websites and IP Addresses
- ☐ Advanced Endpoint Protection Which Stops 99.9% of Ransomware Activity, as a Final Layer of Defense

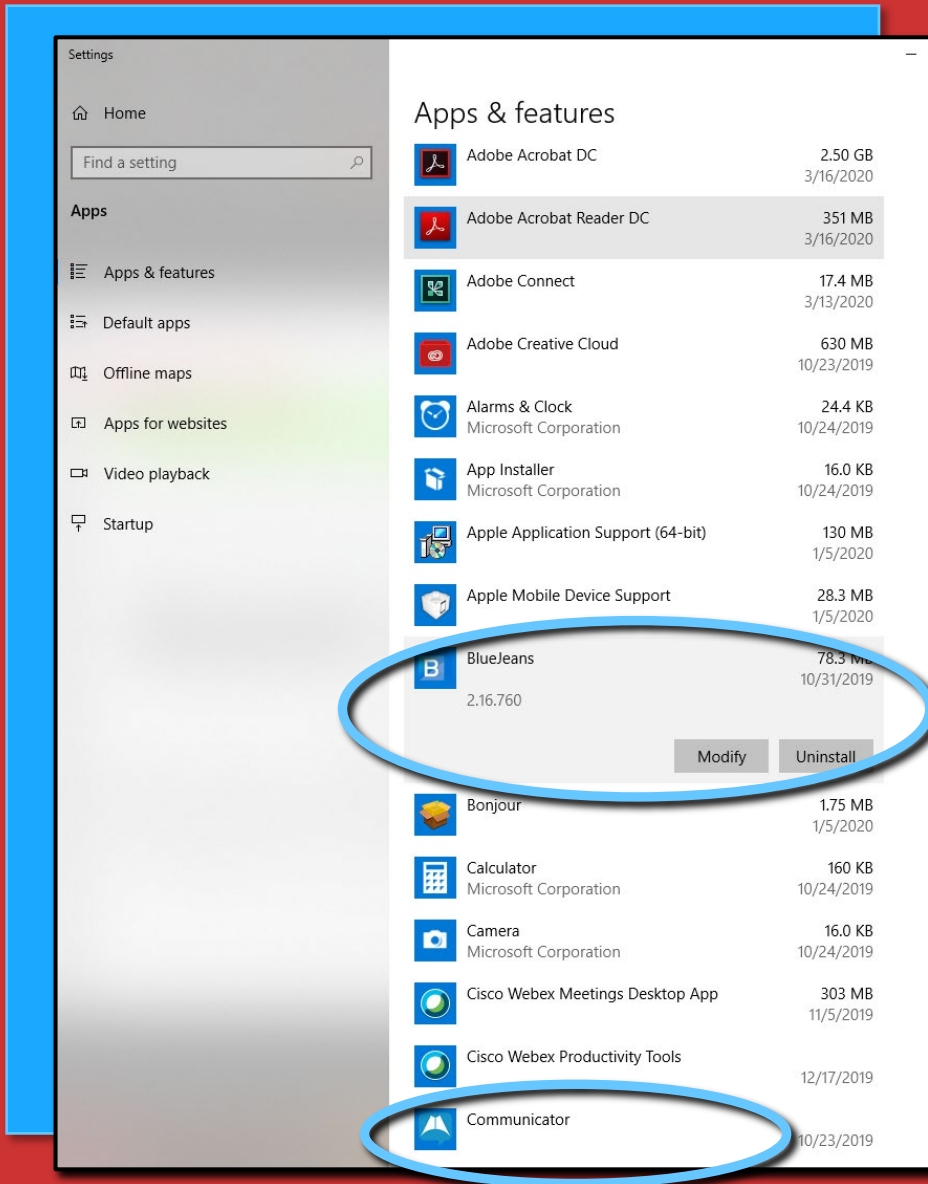


See Something? Say Something



1. If you receive a suspicious email, report it to your IT provider. Others may receive the same email and should know not to action on it.
2. Using the Outlook application at the office, you might have a "Report Message" button that is not available when working on the webpage or a mobile device. Know who to forward the email to, so it can still be reported.
3. Notice a big slow down in your system? It might just be the internet, or an update installing – or it might be something more nefarious. It's okay to ask to get it checked out by IT.

Uninstall Unnecessary Software

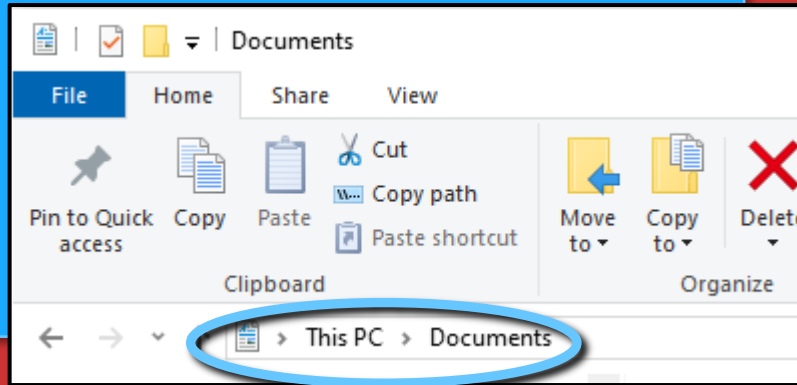


1. Using the Win key on your keyboard, type “programs” and the “Add or Remove Programs” option will come up to the top of the Start Menu.
2. In my case, I saw that I had a few programs that I no longer need. If you click on each program, you get the option to Modify or Uninstall. I Uninstalled Blue Jeans and Communicator.
3. If you’re uncertain which programs are safe to uninstall, ask your IT person for assistance.

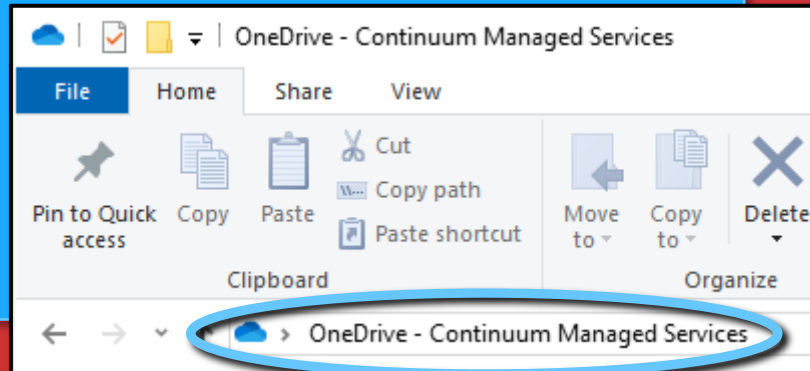
A grayscale background image showing a person from the chest up, wearing a light-colored sweater. They are looking down at a small object, likely a smartphone, held in their hands. The background is blurred, suggesting an indoor setting with a table and other objects.

“What lessons, tips, and any tricks have you learned, with your experiences dealing with ransomware?”

Data Backup



1. Check with your IT Provider to see if data you create or modify is being backed up correctly.
 - A. Cloud applications /repositories may have versioning (saves a copy of each version you work on, automatically) but may not be backed up in a separate location.
 - B. Files you copy to your personal computer may represent a breach in confidentiality or policy. Understand how to access and save data correctly, to avoid any potential problems down the road.



Thank You

Please See Your IT Provider with Questions and Assistance.

1 - "18 Things to Make Your Remote Work Secure, Convenient, and Stress-Free."

1 - "Dark Web Report by domain or email."

1 - "15 Ways to Protect Your Business From A Cyber Attack!"

