

# RedLine

*Storing Passwords in your Browser Can Ruin Your Life  
(But Will Make Criminals VERY Happy!)*

*In a kinder, gentler world, you might be able to store all your passwords and logins in your browser, and it would be safe and convenient. This is not that world; storing passwords in your browser can be extremely risky.*

*Your most significant risks for getting infected with password-stealing malware are sites where you or your children can download games and sites for tricks, tips, and hacks or cracks on gaming (e.g., some YouTube sites).*



By Britton White and "Dissent Doe, PhD

# PART 1

## Understanding the Risk!

In a kinder, gentler world, we might be able to conveniently store all our passwords and logins in our browser and they would be safe. This is not that world; storing passwords in our browser can be perilous.

Info stealers have been around for years. Still, if you have never heard of “info stealer” or have heard of it but have no clue what it is or how it affects you, this article is for you. We will explain in plain English the threat it poses to you, your children’s school, your employer, and even Nana, PopPop, and Great-Aunt Molly.

Let’s start with something you probably already know. By now, most people have heard that it’s an awful, terrible, never-ever-do-this idea to use “123456” as your password for anything. Family members’ names, pets’ names, anniversaries, or birthdates are also frowned upon.



If you want to conduct your banking online, access your medical records online, or do anything involving personal and sensitive information, you need strong passwords to protect your accounts. Some professionals recommend that you use a password that is a long phrase with at least fourteen characters. Some sites may require using a password that meets specific requirements, including uppercase and lowercase letters, numbers, and special symbols.

How will you remember a password if you use a 14-character password that looks like your cat wandered across your keyboard and hit a random string of keys? Remembering or being able to retrieve passwords when we need them is a considerable challenge, and the older we get, the harder it may become. Re-using the same password across accounts is not okay, so you cannot even create one complex password, memorize it, and use it everywhere.

## Not All Solutions Are What They Are Cracked Up to Be!

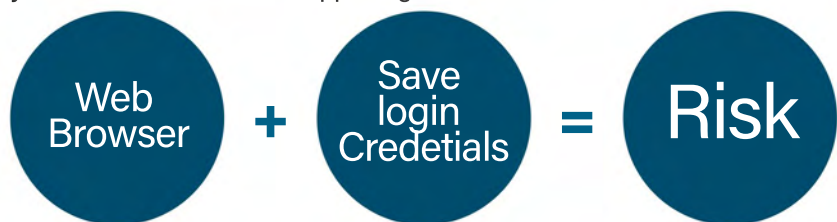
Suddenly, one day, a technological savior appears before you. As you create a new account at a website, a Google popup offers to generate a strong password for you and not only will it create it for you, but it asks you whether you want Google to save that password for you. If you click “SAVE,” Google will store your username and password for that site. The next time you visit that site, Google will autofill your username and password.

# How convenient! How wonderful! Your password creation and storage problem are solved, right?

Not really.

When you allow Google Chrome or any other browser to save your logins so you can autofill logins on sites, you've now put all your login eggs in one basket. All your logins can be stolen if that basket gets hacked or compromised. And that is precisely what happens, time and time again, and usually without our knowledge.

This is not just a Google or Chrome issue. The risk also exists if you use a "password manager" app to create and store your login credentials. While it is convenient to use a password manager that gets added to your browser as an extension, if you visit a site with malicious code, that malicious code can steal a copy of all your stored login credentials. And you won't even know it's happening.



## What Are Info Stealers?

Info stealers are malware (malicious programs) that can infect your files and devices. Often, you will not even know that you have been infected. Still, the malware may be stealing information from your phone or computer and sending it to another server where criminals amass data they can misuse.

How many logins do you have for your accounts? If you start adding up all the logins/accounts you created online for your phone numbers, your email accounts, your banking accounts, your investment trading accounts, Amazon, stores that you shop at online, your health records from your medical providers, your children's school network accounts, and maybe even the account you set up to monitor your accounts for identity theft – how many logins would you have?

## How Do info stealers Gain Access to Your Devices?

There are various ways your devices can become infected. Here are a few of the ways:

- ◆ You receive an unexpected email. It tells you that you need to verify your account, or it will be terminated within 24 hours. You click on the link and go to the site. That site, without your knowledge, can drop malware onto your device. You don't even need to download anything from the site.



Just visiting it can lead to infection. Note: Many browsers will warn you if you try to connect to a dangerous site. If you get a warning suggesting you do not connect to a site, do not connect to it. And teach your children that if they ever see warnings about connecting to a site, they should not connect to it until they check with you about it.

- ◆ You innocently click a popup box to allow notifications from a site you are visiting. Some websites issue false malware alerts to get the individual to click on the alert. The alert sends visitors to websites where their information is gathered/stolen.
- ◆ Downloading games from the Internet or looking up hacks or cracks on sites such as YouTube may result in you or your child downloading a hack or crack that contains a malicious executable file.

## The “RedLine” Info Stealer.

RedLine is one type of info stealer. We are using it as an example to show the risks you face if you store your login credentials in your browser or a password manager installed in your browser.



## Getting Schooled on RedLine

In his research, Britton found a university student with credentials to 531 sites stolen from their Chrome browser by RedLine.

Britton tracked the student down and contacted them to alert them that all their logins had been stolen and were up for sale on the dark web. But Britton also looked deeper into the situation. From the student's login credentials, it appeared that this student had part-time employment with his university and used his computer to access his work account on the university's domain.

*Apart from criminals now being able to log in to more than 500 of his accounts, anyone who bought or obtained the credentials might have been able to access whatever university data was accessible to the student in his employment.*

In this case, the student, when contacted, mentioned that he knew he had been hacked at some point. But did he ever tell his university so that they could check to determine if anything he had access to had been accessed illegally? Should he have told them? And should the university have had a policy that required employees to notify them of any security compromise of personal devices used to access their work account(s)? We'll get to those thorny questions in Part 2 of this article.

As fate would have it, as we were working on this article, Cisco, a multinational technology firm, announced it had been the victim of a ransomware attack. Cisco forthrightly admitted that the attackers gained

access when an employee's login credentials were compromised by an attacker gaining control of the employee's personal Google account, where credentials saved in the employee's browser were being synchronized.

Curious, we ran a search and found six people who had Cisco login credentials stolen by an info stealer. Some may be current employees, some may be former employees, and at least one was an employee of a partner firm who had both his login to his firm and his login to Cisco stolen. Note that we are not saying that any of these were related to the Cisco breach, but it is a reminder that login credentials are easy to steal, and firms should require more than just a username and password to log in.

## Doctor, Doctor, Give Me the News

Because both authors focus on the healthcare industry, Britton also looked for examples from healthcare. Here is just a very tiny Redline sample of what could be found, redacted by us:

### American Medical Association Logins:

1. URL: <https://login.ama-assn.org/account/login>  
Username: T\*\*\*\*\*02  
Password: B\*\*\*\*\*15
2. HOST: <https://fsso.ama-assn.org/login/account/login>  
USER: k\*\*\*\*\*c  
PASS: M\*\*\*\*\*9

### American Dental Association<sup>2</sup>:

HOST: [https://dts.ada.org/login/login\\_\\_ADA.aspx](https://dts.ada.org/login/login__ADA.aspx)  
USER: 6\*\*\*\*\*4  
PASS: M\*\*\*\*\*3

### NYU Langone Health:

URL: <https://mail.nyumc.org/owa/auth/logon.aspx>  
Username: r\*\*\*\*\*2  
Password: O\*\*\*\*\*0\*  
Application: Google\_[Chrome]\_Profile 2

### Washington University School of Medicine<sup>3</sup>:

URL: <https://cecvpn.seas.wustl.edu/+CSCOE+/logon.html>  
Username: z\*\*\*\*\*g.\*\*\*g  
Password: \$\*\*\*\*\*6  
Application: Google\_[Chrome]\_Profile 1

### Washington University School of Medicine:

URL: <https://connect.wustl.edu/login/wulogin.aspx>  
Username: z\*\*\*\*\*g.\*\*\*g  
Password: r\*\*\*\*\*V  
Application: Google\_[Chrome]\_Profile 1

<sup>2</sup> The American Dental Association suffered a ransomware attack by Black Basta this year. We do not know whether any login credentials stolen by RedLine or another info stealer may have been exploited to gain access.

<sup>3</sup> We do not know if the compromised credentials were responsible or related to this ransomware attack, either. Still, we will point out that the high risk is a good reason for people to use two-factor authentication for their important account logins.

# Your Logins, For Sale

RedLine info stealer logs can be found for sale on underground forums and even on clearnet sites.

Thread / Author	Forum	Replies	Views	Last Post (and)
REDLINEVIP PREMIUM 1037 MARCH LOGS 2022 [part 1] ( 1 2 ) Usa	Stealer Logs	25	5,357	41 minutes ago Last Post: RALPHJEET
LOGS 2022   #7 : whitenigger	Stealer Logs	5	375	6 hours ago Last Post: shmedouch
SELLING CLOUD WITH MORE THAN 1,000,000 LOGS APRIL-JULY 2022 ( 1 2 ) BrodMax	Leaks Market	18	587	7 hours ago Last Post: BrodMax
147GB Redline Logs Mixed 2022 pachel	Stealer Logs	5	292	7 hours ago Last Post: shmedouch
CLOUD WITH MORE THAN 480,000 LOGS JUNE-AUG 2022 ( 1 2 ) BrodMax	Leaks Market	12	596	Yesterday 02:00 PM Last Post: BrodMax
LOGS 2022   #10 : whitenigger	Stealer Logs	4	523	August 16, 2022, 08:28 PM Last Post: S0ul
Free june redline logs - 1k r4d10n5	Stealer Logs	5	1,143	August 16, 2022, 03:19 PM Last Post: exploitaz
USA Logs from Redline 137Mb buffbyte	Stealer Logs	3	808	August 15, 2022, 11:35 AM Last Post: D4W0
Best stealer to buy? sawp0use	The Lounge	4	164	August 14, 2022, 06:19 AM Last Post: sawp0use

Fig. 1. Info stealer logs with thousands or millions of login credentials can be found for sale or free sharing online in hacking-related forums or Telegram channels. Savvy criminals can search

*For logins for specific victims or targets. These listings were posted on a popular hacking-related forum that is not even on the dark web – anyone can access it.*

Think about it: if you get compromised by malware that steals your login credentials, and you work from home and log in to your work domain and account from home, what will criminals be able to access?

Still not scared? Consider the answers to these questions in this little Frequently Asked Questions (FAQ) we created for you:

**Q: “I have up-to-date antivirus (AV) software enabled on my computer. Will that detect an info stealer and block it?”**

A: Your antivirus software may say it has stopped the malware, but Britton’s research has found specific anti-virus/anti-malware products like Windows Defender, Malwarebytes, Norton, and McAfee do not stop the exfiltration of saved browser credentials.



**Q: “My child uses our family computer to browse the internet for homework. Are we safe if they browse but don’t log in to any site?”**

A: Is your child old enough or computer savvy enough to understand and respond appropriately if they attempt to visit a site and their browser displays a warning? Or will they go ahead and connect anyway? Frequently Asked Questions (FAQ) we created for you:

**Q: Is there any way to check to see if I am infected with RedLine or another info stealer?**

A: Sadly, there is no easy way for the average consumer to find out. While antivirus software is not a perfect defense against infection nor an ideal detector if you have been infected, use it and set it to update automatically whenever a new version or update is available. Also, periodically run scans of your computer system.



Q: If I discover that I was infected with an info stealer and had a login to my child's school stored, am I putting the school district's security at risk?"

A: Depending on what that login would enable attackers to access, you may be. Remember that threat actors can often escalate or branch out from the point of access once they get into a system.



Q. Could this get any worse?

A: Sure.

Nightmare #1: There have been many instances where the home router/modem/firewall has been compromised because the username and password for the device had been stored in the browser. When this happens, your whole network has been compromised.

Nightmare #2: Your account is taken over by criminals who then pose as you to phish or scam your friends and family.

Nightmare #3: You signed up for Experian's services due to a previous data breach. Now your login to Experian gets stolen by RedLine, and you don't even know it has happened. Whoever buys your RedLine logs can access your Experian account and all the personal and sensitive information it has about you. Experian doesn't offer two-factor authentication for security on logins to their service.

*On July 11, 2022, ID.me announced, "ID.me, the secure digital identity network, today announced a new milestone of around 12.5 million users from the military community. These users have used ID.me's login, which makes digital identities reusable, 253 million times to access benefits from government, non-profits, and private organizations."*

As you can see below, we've provided a redacted set of compromised credentials for a military member. their service.

1. 

URL: <https://www.id.me/users/sign-in>  
Username: \*\*\*\*\*cooke\*\*\*\*\*@gmail.com  
Password: Tlc12345  
Application: Google\_[Chrome]\_Default
2. 

URL: <https://myaccess.dmdc.osd.mil/identitymanagement/authenticate.do>  
Username: \*\*\*\*\*cooke  
Password: |\*\*\*\*\*\$  
Application: Google\_[Chrome]\_Default

There are many more like this individual who has been compromised. We do not know if sensitive military information has been compromised because any military personnel has been hit with the RedLine info stealer. We do know, however, that members of the military may use their military email addresses for some non-military accounts. Military personnel, civilian contractors, defense contractors, and any other organization with ties to the military must understand the consequences of a personal breach that could potentially impact many others.

A quick search of the Cyber Awareness Training login URL for the Information and Communication Technologies Defense (ICTD) Division yielded the following:

URL: <https://federation.eams.army.mil/sso/authenticate/>

Username: b\*\*\*\*\*peters

Password: @\*\*\*\*\*@

Application: Google\_[Chrome]\_Default

Maybe they know, for example, that they should implement two-factor authentication on email accounts, financial accounts, and other sensitive/critical web-based accounts. We certainly hope so<sup>4</sup>. We contacted ID.me to ask whether they require the use of 2FA, but they didn't respond.

## An Ounce of Prevention....

Steps you can take to minimize chances related to info stealer compromise:

1. Don't allow Google Chrome, Microsoft Edge, or any other browser to store your logins for you.
2. Make a list of all your credentials and keep it somewhere where it's not obvious to spot, but you will remember where to find it if you need it. Make sure a family member or executor of your estate will know where to find your list of logins. Update that list periodically because, of course, you should change passwords occasionally.
3. Check on HaveIBeenPwned.com to see if any of your login credentials have shown up in any data breach on their site. If they have, change your credentials for any site where your credentials were breached. Also, change your credentials for any other site using those same credentials.
4. Do NOT use the same computer for gaming or videos that you use for work-related accounts, personal finance/banking, your children's school network, taxes, your patient portal for your health records, or anything personal and sensitive. Use a separate device for any online games or videos, etc.

## If You Discover That You Have Been Infected

1. If you discover that your computer or device is infected, disinfecting it is a priority. Removing malware is not for the faint-hearted, though; you may need to hire a professional. In the meantime, if you can access your accounts from another computer or device you are sure is not infected, change your passwords on your important accounts. If you cannot access your accounts from a safe (non-infected) device, you may have to wait to change your passwords until after you disinfect your device.
2. If you had full credit card numbers stored that may have been captured by the info stealer, you should alert your bank or credit card company to flag your account number for monitoring. And please let us take this opportunity to remind you never to shop online using your debit card. You will have more protection if you use your credit card number if your card number is stolen and used for fraud.
3. For old accounts that you no longer need, go to those sites, log in, and delete the accounts.
4. When you are done changing passwords and deleting accounts, go into your browser settings and clear all cookies and all data.

You can find directions for how to do this for Chrome at:

<https://support.google.com/chrome/answer/2392709?hl=en&co=GENIE.Platform%3DDesktop>



# PART 2

## Now About Those Work Accounts...

When Britton first wrote about this issue on LinkedIn, he offered some recommendations for employers. But of course, we are not lawyers and have learned the life lesson that just because something makes sense to us doesn't make it legal.

*Joseph J. Lazzarotti is a principal in the Berkeley Heights, New Jersey, office of Jackson Lewis P.C. He founded and currently co-leads the firm's Privacy, Data, and Cybersecurity practice group, edits the firm's Privacy Blog, and is a Certified Information Privacy Professional (CIPP) with the International Association of Privacy Professionals. Trained as an employee benefits lawyer focused on compliance, Joe also is a member of the firm's Employee Benefits practice group. Joe's Workplace Privacy, Data Management & Security Report is on our daily to-read list.*

In considering his answers, note that they are in the context of U.S. law. Even with that proviso, different states may have different laws. The following is from a Q&A email exchange between Dissent Do ("DD") and Joseph Lazzarotti ("JL"), edited only lightly:

**DD:** What do you think about running a search on a prospective employee's primary and secondary email addresses to see if those email addresses have ever shown up in any known data breach?

**JL:** I believe this would be a prudent risk management measure. However, there are several issues employers should consider before adopting this approach. Here are some examples:



**First**, they should assess with counsel whether this search constitutes a background or similar check that might require notice and/or consent, particularly if they use a third-party vendor to conduct the search.

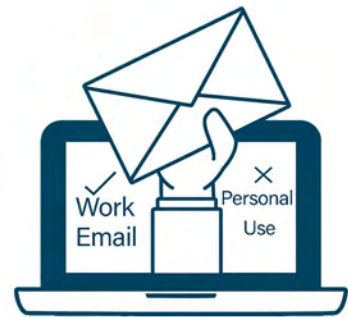
**Second**, employers should consider what to do with the personal email addresses once collected, such as safeguards, retention, further use or disclosure, etc.

If a third-party service provider is assisting with the administration of this search, the service provider should be subjected to the employer's vendor assessment program.

**DD:** What about prohibiting hired employees from using their work email addresses for personal use?

**JL:** In general, I believe this is a prudent policy. Practically, however, it can be difficult to implement and enforce. Some factors may make workers more likely to use their work email address - personal versus professional engagement in social media is often blurred, and the convenience of having one email to use for managing multiple online accounts is compelling. There also could be difficulties with enforcement. Absent

some inquiry or audit, including an attempt, perhaps by someone in HR, to log into personal accounts using company email addresses (which presents a significant legal risk, including civil and potential criminal penalties), how would companies know their email addresses are used in this matter?



Perhaps dark web searches could provide helpful information, but that process could be time-consuming and expensive. Such an inquiry or audit could be problematic in about half the states as they could involve asking employees what the credentials are for their personal online accounts, including if they are company email account accounts. This is because those state laws generally prohibit such requests.

Another concern involves the back-and-forth of labor law. Under the National Labor Relations Act, employees (including non-union employees) have a right to engage in “protected concerted activity” – that is, very generally, communications with other workers about working conditions, pay, benefits, etc. In 2014, in a case called *In re Purple Communications, Inc.*, the NLRB found that employers that provide employees with access to their email system could not prohibit using those systems for protected concerted activity. The composition of the Board at that time of that case has changed, relaxing the holding in *In re Purple Communications, Inc.*, but the new administration may change that again.

Of course, I realize this is not the “use” you are considering; your focus is on the use of the business email addresses themselves. However, care is needed when drafting these policies to avoid allegations of a chilling effect on protected concerted activity.

**DD:** Can an employer ask a potential employee if their information has ever been caught up in a data breach?

**JL:** In general, I am not aware of a proscription against such an inquiry. However, the employer may receive information in the response that it did not expect and does not want. For example, HIPAA and several state breach notification laws include medical information in the definition of personal information that, if breached, could require notification to affected persons. So, in response to such a question, an employee might respond, “Yes, my [therapist, oncologist, etc.] was hit with a ransomware attack” or some variation, which also could include information



**DD:** Can an employer ask a potential employee if they use two-factor or multi-factor authentication for their personal accounts?

**JL:** Yes. Note that for these and other questions, we have answered based on US law. There could be limitations in other jurisdictions that might affect whether or how such requests are posed, such as under the General Data Protection Regulation in the EU.



**DD:** Can an employer ask a potential employee if they store login credentials in their browser or if they use a password manager?

**JL:** Yes, however, note that some employees may not realize whether they are doing so. So, if such a request is put to employees, instructions on how to check might be provided to help obtain more accurate answers.

**DD:** If an employer allows users to login into any related work environment from personal devices, can the employer mandate that if the employee becomes aware of malware or breach of any device used to access company resources, they must notify the employer promptly? Can they require employees to run periodic searches on their email addresses to see if their email addresses have shown up in any breaches?

**JL:** Yes. We have helped many employers establish "Bring Your Own Device" policies which allow, among other things, employees to access company email and other services using their personal devices. Under these policies, and in exchange for obtaining access, employees can be asked to agree to certain conditions. Typically, one of those conditions is a requirement to notify the employer in the event of a breach of the device.

**DD:** Could doing any of the above violate labor or workplace privacy laws?

**JL:** See above. And, yes, there can be other issues that need to be considered depending on the circumstances. These include: (i) if applicable, making sure personal information collected for these purposes is reflected in the notices at collections for employees and/or applicants under the California Consumer Privacy Act; (ii) determining whether the employer is engaged in electronic monitoring and whether notice is required, and (iii) using the information for purposes other than improving security.

**DD:** Is there anything I haven't asked you that you wish I had asked you about this topic?

**JL:** What is personal use? Does it include using the company email address when setting up an account with the vendor managing the company's 401(k) plan or some other employee benefit? What if the employee is also going to school for a job-related degree?



Great thanks to Joe for shedding some light on the issues and potential pitfalls and for reminding us that employees may not know when their credentials have been compromised or know how to check to determine if they have been compromised. Joe's suggestion that employers provide employees with instructions on how to check to see if they are storing credentials in their browser or a password manager is a somewhat chilling reminder that many people have no idea what they are doing or what they may have done.



## What about HIPAA and HITECH?



HIPAA and HITECH impose security and privacy rules on covered entities. We asked Matt Fisher of Carium whether those regulations might change how employers in the healthcare space address info stealers and personnel issues.

*Matt Fisher is General Counsel for Carium, a virtual care platform company. He is responsible for all legal functions in the company and helps to ensure that operations meet the requirements of applicable healthcare laws and regulations. Matt works to find creative solutions when needed and keeps an eye on the complications that can come up from working in the healthcare industry. Prior to joining Carium, Matt practiced for over a dozen years at a mid-size Massachusetts law firm, where Matt advised clients across the healthcare spectrum on healthcare laws and regulations as well as general business matters.*

**DD:** Let me start by asking if you generally agree with Joe Lazzarotti's answers about workplace issues. Given what employees in the healthcare space may have access to, is there any more pressure or need for employers to screen employees or potential employees for breaches involving their personal devices?

**MF:** Joe's responses provide a very good framework for considering the interaction between an employer and an employee. While HIPAA does introduce additional compliance considerations in the healthcare industry, it does not change the basics of labor and employment law that Joe covered. Healthcare adds some layers on top and likely heightens some of the concerns involved, but it does not fundamentally change any of the requirements or restrictions mentioned by Joe.

**DD:** Is there anything Joe said you strongly disagree with as it might apply to the healthcare sector and HIPAA?

**MF:** I don't disagree with anything Joe said, but I think healthcare organizations may want to take a few additional steps. None of the difficulties discussed by Joe go away in healthcare, but HIPAA can provide some influence over other actions to take or implement that could help enhance security.

For example, the Security Rule under HIPAA calls for only enabling access

to information that an individual needs to perform their job. That means someone who has no patient interaction or need to review patient data should not have a login that grants unfettered access to all data stored in the system. Even when an individual needs to view patient information, it may be only for a single department or a specific subset of patients. Considering job-required access is important for segmenting the network and limiting the impact when an account is compromised.

**DD:** HIPAA defines a reportable breach as “The acquisition, access, use, or disclosure of protected health information in a manner not permitted which compromises the security or privacy of the protected health information.” Login credentials are not protected health information. Does this mean that under HIPAA, there is no requirement that an employee or business associate report the theft of their credentials to the covered entity?

**MF:** As noted, HIPAA defines a breach by looking at the impact on protected health information. Not to minimize the impact of login credentials being stolen, but login credentials are not protected health information (at least in most likely scenarios). Since login credentials, in most cases, will not constitute PHI, no breach notification just for the theft of the login credentials would be required. However, the story should not stop there. If login credentials are compromised, the covered entity must start an investigation to look for any network intrusion or other action that could impact PHI. The ability to get into the network creates the very real possibility that a breach could result from the login being taken.

A related consideration is that compromised login credentials likely constitute a security incident that requires a response under HIPAA. While a security incident differs from a breach, it calls for a covered entity to respond and mitigate the impact or potential impact. Notification to individuals will likely still not be called for, but it will push a covered entity to review security practices and make changes.

**DD:** Playing Devil’s Advocate here, suppose an employer does what Joe suggests but an employee knowingly fails to notify the employer that their login credentials were stolen. Assume there is no two-factor authentication for the credentials. The covered entity has a breach. Lawsuits follow, of course. Will the entity likely have more liability for not having two-factor authentication when it knows that employees are using personal devices to connect to work?

**MF:** The question has many components and raises many sidepaths to pursue before being able to quantify any potential liability. Taking the most basic approach first, though, would liability increase just because no two-factor authentication is used despite employees using personal devices? The impact on liability is very hard to know. First, any liability under HIPAA would require the HHS Office for Civil Rights and/or a state attorney general to investigate and pursue a fine after a breach. It is important to remember that a very small portion of breaches results in an organization being fined or entering into a settlement. Further, when fines or settlements occur, it is usually the result of finding that the organization had other areas of non-compliance that showed systemic failures. That is the quick, high-level assessment under HIPAA.

It is also necessary to consider state law, which will vary by state. Following many data breach notifications, an individual or group of individuals will sue the impacted organization under state law theories for impacts on privacy. The lawsuits will seek recovery for time spent monitoring identity theft or other issues and speculative damages for the emotional impact. The exact increase in liability is not clear, though, as the lawsuits seem to either be dismissed for failure to state direct damages or settle in a way that can best be identified as resolving a nuisance.

Getting back to the root of the question, though, it is hard to state one way or the other that not implementing two-factor authentication would directly result in increased liability. It will all depend on the facts and circumstances and the applicable law.

**DD: Are you aware of any data breaches in the healthcare space due to credentials stolen from an employee's personal device?**

**MF:** No specific example jumps to mind of a healthcare data breach resulting from credentials being stolen off an employee's personal device. Just because an easy example does not jump to mind, though, it does not mean that that scenario has not happened. Given all the breaches reported resulting from email compromise or detection of suspicious network activity, there is a high likelihood that credential theft from a personal device has occurred. Not only has it likely happened, but it has likely happened much more frequently than expected.

**DD: What advice do you give employers that allow or require employees to use their personal devices for work?**

**MF:** If an employer permits use of personal devices, it is very important to have a policy governing the use of personal devices. Joe mentioned having what is commonly called a "Bring Your Own Device" policy, which sets expectations, obligations, and limitations. Being clear in internal communications helps set the baseline for what needs to occur and establishes a base from which the employer can take action.




Beyond a BYOD policy, an employer could explore a mobile device management (MDM) solution that could isolate the employer's data on the personal device and/or give the employer the ability to remotely wipe a device in case of a compromise or other issue. From personal experience, an MDM tool can be quite powerful. The one I had experience with prevented data from being downloaded onto my personal device, which minimized the potential impact of the device being lost. The MDM tool also required a separate login to access work information even once my device was unlocked, adding another layer of protection.

**DD: Is there anything I haven't asked you that you wish I had asked you?**

**MF:** A good question is, what can an organization do to increase compliance with security efforts? The answer is somewhat multipronged





but goes to education, awareness, and culture. Security has to start from a place of knowledge, which can only occur with consistent education and promoting awareness of emerging or changing threats. At the same time, an organization needs to create and cultivate a culture that takes security seriously from the top down. It is doubtful that all security attacks can be stopped, but how quickly mitigation can start is important in minimizing the impacts.

As always, Matt raises some excellent points. And if the people at the top of the organization are unaware of the risk of info stealers, as one example, how does that impact their ability to develop workplace policies related to the use of personal devices and whether the employees' devices should be routinely screened for signs of malware or other security risks? As Matt suggested, a culture of security has to start from a place of knowledge.

## Conclusion

RedLine info stealer is just one of many types of info stealers. Password manager apps, when open and in use, put all stored logins at risk of compromise by malware. One password, even a strong or complex one, is not enough to really secure your important accounts. Use two-factor authentication or multifactor authentication to add additional protection so that even if your login credentials are stolen, the bad actors will still not be able to access your account.

We believe this bears repeating: do NOT use the same computer for gaming or videos that you use for work-related accounts, personal finance/banking, your children's school network, taxes, your patient portal for your health records, or anything personal and sensitive. Use a separate device for any online games or videos, etc.

# About the Authors



## Britton White:

has spent six years in healthcare compliance and security conducting risk assessments for hospitals and health systems around the country. His focus on Open-Source Intelligence (OSINT) and dark web research led to his better understanding of info stealing malware. In February of 2022, he began to notify victims around the country that they and/or their employees' saved browser credentials had been stolen.

## Dissent Doe, PhD:

is a licensed psychologist. In 2006, she opened "PogoWasRight.org" to raise public awareness of privacy issues. In 2009, she opened a second site, DataBreaches.net, to report and comment on data security lapses that put individuals' privacy at risk. Breaches in the healthcare and education sectors remain her priorities.



*This article was written by Britton White and "Dissent Doe, PhD" in August 2022. It was originally published on PogoWasRight.org under a Creative **Common Attribution-NonCommercial-ShareAlike 4.0 International License**. If you republish it, we ask that you credit the authors and preserve this licensing notice.*