



CYBERSECURITY

AWARENESS MONTH

2022

GABRIELLE DECKER | OKLAHOMA CITY COMMUNITY COLLEGE

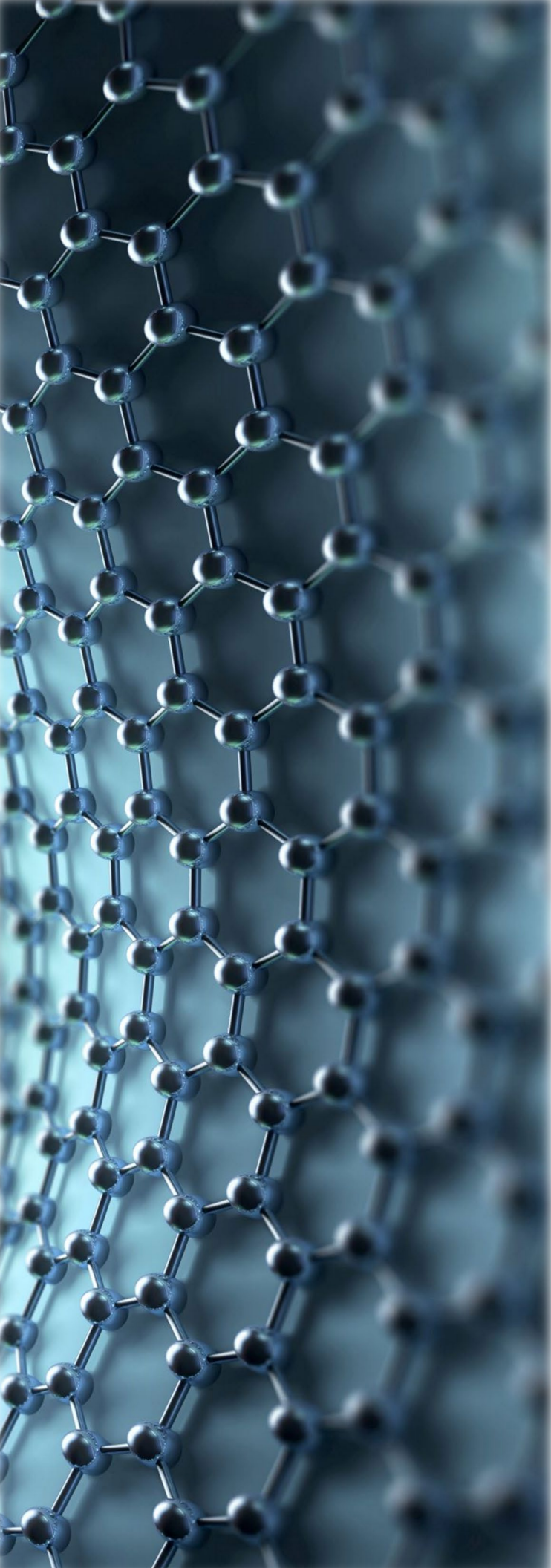


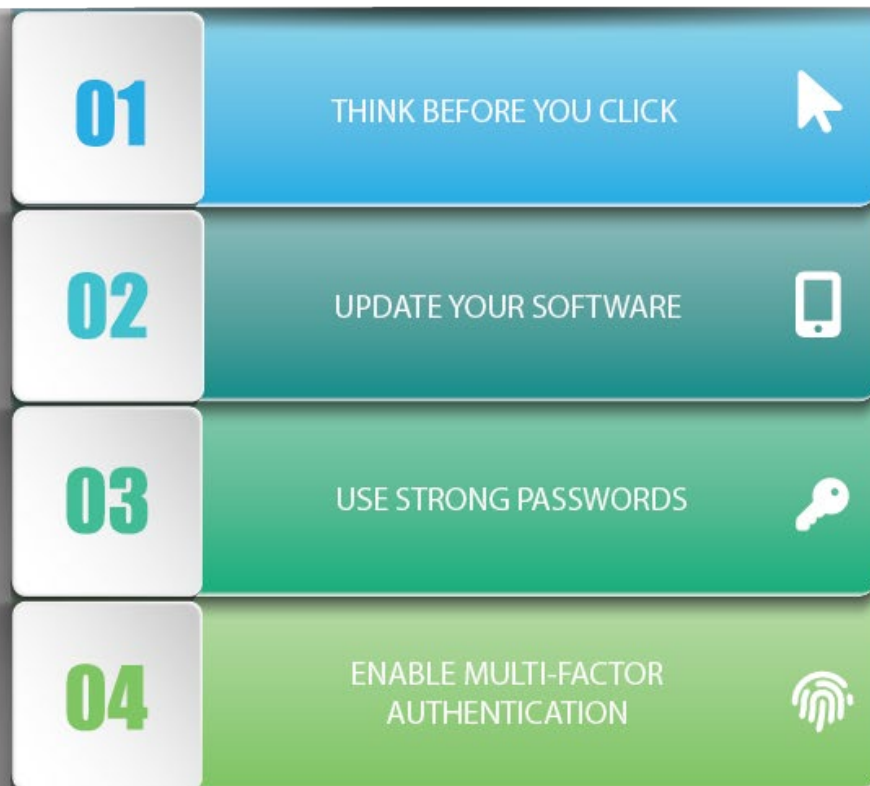
TABLE OF CONTENTS

Introduction	3
1. Think before you click.....	5
2. Keep your apps and devices up to date	7
3. Use strong passwords.....	8
4. Use two- or multi-factor authentication	9
5. Install anti-malware software.....	10
6. Be cautious about what you post online.....	11
7. Do not store passwords or credit cards	12
8. Be cautious with public wi-fi	13
9. Create a secure email	14
10. Monitor your credit	15
How to report a cybersecurity incident.....	16
Cybersecurity resources.....	17
References	18


INTRODUCTION

October is Cybersecurity Awareness Month, a joint federal effort spearheaded by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA). While cybersecurity may appear to be a complex subject, the campaign theme for this year, "See Yourself in Cyber," shows that it is, in the end, all about people.

Throughout the month of October, CISA and NCA will shine a spotlight on essential moves that everyone can make:



As the world becomes more digital, our lives are more interconnected than ever before. Unfortunately, this increases our vulnerability to cybercrime. Cyberattacks are becoming more sophisticated and common, and the consequences can be disastrous. According to IBM, the average cost of a data breach was \$4.24 million in 2021 [1], the highest average on record. Sadly, the likelihood that a cybercriminal is detected and prosecuted in the U.S. is estimated at around 0.05 percent [2]. This means that most cybercriminals get away with their crimes.



While the internet offers many benefits, it also comes with risks. Hackers and cybercriminals are constantly finding new ways to exploit vulnerabilities and steal personal information. Despite this, many people are still unaware of the dangers of cybercrime. According to a recent Varonis survey, 64 percent of Americans have never checked to see if they were affected by a data breach, and 56 percent are unsure what steps to take in the event of one [3]. Did you know that 95 percent of cybersecurity breaches are caused by human error [4]? Or that 94% of malware is distributed via email [5]? This means that we all need to exercise extreme caution so that we don't add to the problem.

COVID-19 has also made us more vulnerable to cybercrime. In 2020, Americans lost more than \$97.39 million to COVID-19 and stimulus check scams [6]. To make matters worse, hackers are exploiting the pandemic to launch attacks on already overburdened healthcare organizations. According to Forbes, hackers attack an average of 26,000 times per day [7]. Their attacks are becoming more sophisticated and difficult to detect, and hackers are now using artificial intelligence to launch attacks.

This booklet is designed to raise awareness of the dangers of cybercrime and to help you protect yourself and your loved ones. It includes information that aligns with this year's "See Yourself in Cyber" campaign theme, as well as information on the most common types of cyberattacks, the steps you can take to prevent them, and what to do if you are a victim of one. The goal is to empower you to take control of your cybersecurity and protect yourself and your data from cyber criminals.

For more information and resources on cybersecurity, visit the website for [Cybersecurity Awareness Month](#).



1. THINK BEFORE YOU CLICK

In today's age of digital information, it's important to be aware of the dangers of clicking on links or attachments from unknown senders. While the internet has made it easier than ever to connect with people and information, it's also made it easier for scammers and cyber criminals to commit fraud. Hackers become experts in social engineering, which is the art of using human psychology to exploit vulnerabilities. They will tailor phishing attacks to known interests that can be used to trick you into disclosing credentials, clicking a malicious link, or opening an attachment that infects your system with malware.

Suppose you recently conducted several searches for inexpensive auto insurance. Hackers may devise an attack disguised as an email or text message claiming to offer you a special discount. You click on the link or open the file, at which point a hidden script within the file activates and opens a back door into your system. The hacker can then access your computer at any time and view your screen. All the login and credit card information you enter will be displayed. They can activate your camera and microphone to take photographs and eavesdrop on your conversations. The goal of the phisher is to collect this sensitive information, which they could use to commit identity theft or financial fraud. To put it in perspective, **47 percent of Americans experienced financial identity theft in 2020** [8].

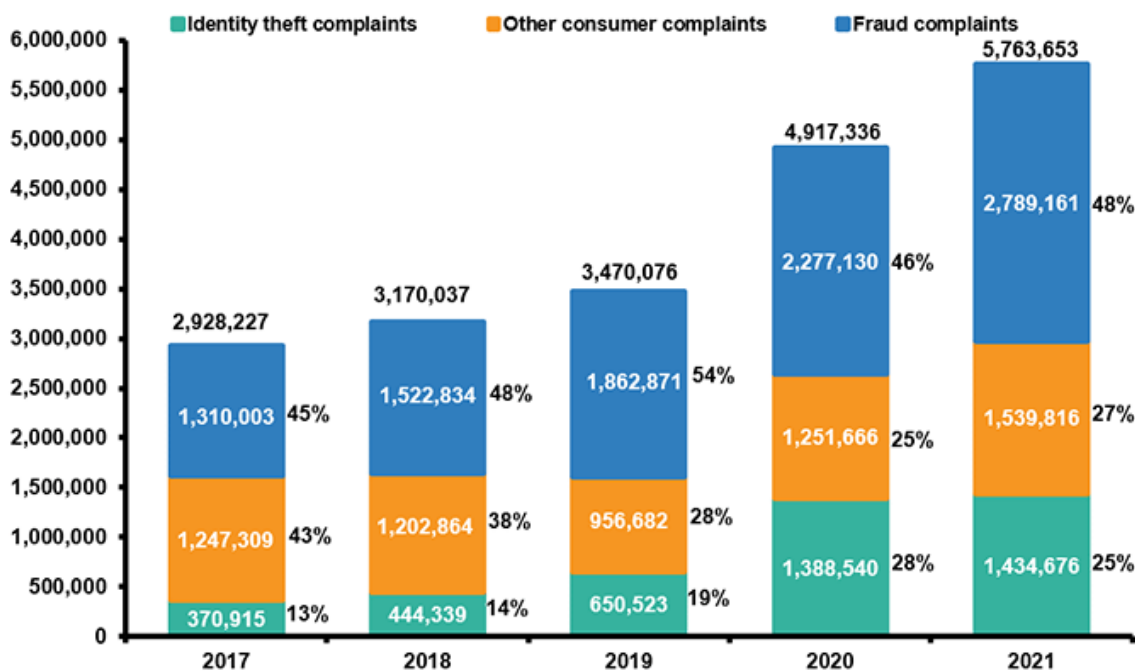


Figure 1 Percentages are based on the total number of Consumer Sentinel Network reports by calendar year.
Source: FTC, Consumer Sentinel Network.



If you receive an email from an unknown sender, the best thing to do is to delete it immediately. Don't click on any links or attachments, even if they look harmless. Remember, it's better to be safe than sorry when it comes to your personal information.

2. KEEP YOUR APPS AND DEVICES UP TO DATE

It's important to keep your software and devices up-to-date for a number of reasons. New updates often include security patches that fix vulnerabilities that could be exploited by malware. If you don't update your software, you leave yourself open to attacks. Additionally, updates can improve the performance of your devices and software and fix any bugs that might be causing problems.

Turn on automatic updates so that your device will automatically install updates when they become available. Update all your applications, too - especially your web browsers. Most software will automatically check for updates, but it's a good idea to check manually as well.



Windows

1. To check for updates on Windows, go to the Start menu and select "Settings".
2. Then, click "Update & Security" and select "Check for updates".

If there are any updates available, they will be downloaded and installed.



Apple

1. To check for updates on a Mac, click the Apple menu and select "Software Update".
2. If there are any updates available, they will be downloaded and installed.



Android

System updates usually send notifications to your device when an update is available. However, it's still a good idea to check periodically.

1. Open the Settings app, scroll down and tap System.
2. Tap Advanced, System Update, and then Check for Update.
3. Tap Install if an update is available. Restart if prompted.

To update your apps, which happens much more frequently:

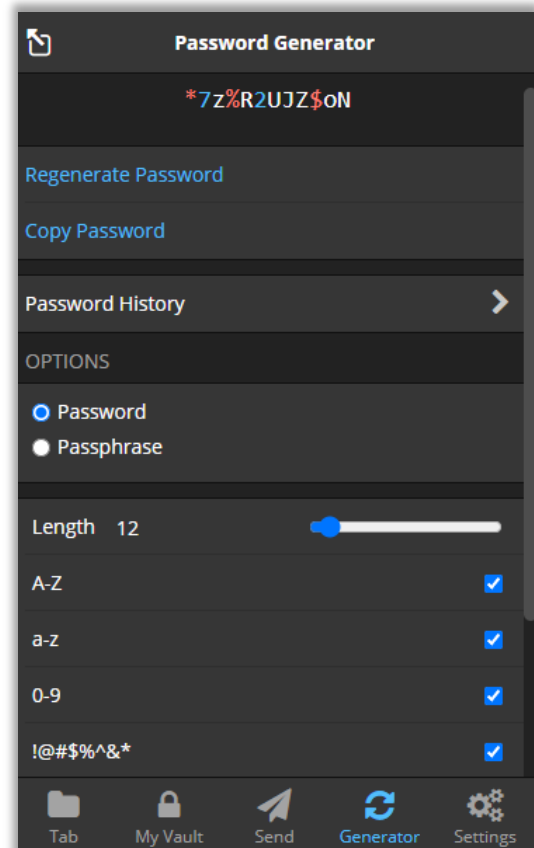
1. Open the Google Play Store app.
2. Tap Menu, then My apps & games.
3. Apps with an update available are labeled "Update."
4. Tap Update All to update all apps. For individual apps, find the specific app you want to update and tap Update.

3. USE STRONG PASSWORDS

...and don't re-use them! As a rule, avoid using the same password twice and change it once per year. Include a mix of uppercase letters, lowercase letters, numbers, and special characters in a minimum 12-character password. 15 is preferable. Avoid creating passwords that contain personal information that others may already know or would be simple to discover (e.g., birthdays, nicknames, anniversaries). Hackers search for any data that could be used to guess passwords.

Also, avoid using dictionary words such as "ilovemylife" and patterns such as "abc" or "123" because a hacker can "brute force" passwords containing these words or patterns. Automated brute-force attacks try far more passwords than a human could, breaking into a system by trial and error. Dictionary attacks are more targeted brute-force attacks that use a list of common passwords to speed up the process. This is often the first attack a hacker will attempt against a system, using this technique to check for weak passwords.

"123456" was the most used password in 2020, followed by "123456789" [9]. Attackers can succeed 50% of the time by simply trying the first 25 most common passwords. **A hacker will brute force crack a 10-character password in 3 days. A 15-character password will take 3 million years to crack** [10]. Use a password management tool, such as [Bitwarden](#), to keep track of all your passwords. It has a password generator to create strong passwords for you, and best of all, *it's free*. The screenshot above is an example of a good password generated by Bitwarden. Bitwarden is compatible with iOS, Windows, and Android devices. It can also fill in your passwords for you on each site!



Don't keep your passwords on sticky notes, mobile devices, or other files that a hacker could access. If they are able to access your mobile device's file system, you easily gave them access to all your accounts!

4. USE TWO- OR MULTI-FACTOR AUTHENTICATION

Two-factor authentication (2FA) provides an additional layer of protection for online accounts. When 2FA is enabled, users must provide two pieces of evidence (or "factors") to verify their identity before account access is granted. The most prevalent type of 2FA combines something the user knows (such as a password) with something the user has (such as a code generated by an authentication app). With multi-factor authentication (MFA), you would be prompted to enter more than two additional authentication methods after entering your username and password.

2FA can help prevent unauthorized individuals from accessing user accounts, even if they have the user's password. It can also protect users from being tricked into divulging their passwords.

Google reported in 2019 that 2FA can prevent 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks. In addition, the report found that 2FA prevents 99% of account hijacking attempts [11]. Microsoft asserts that MFA can increase the level of security by 99.99% [12]!

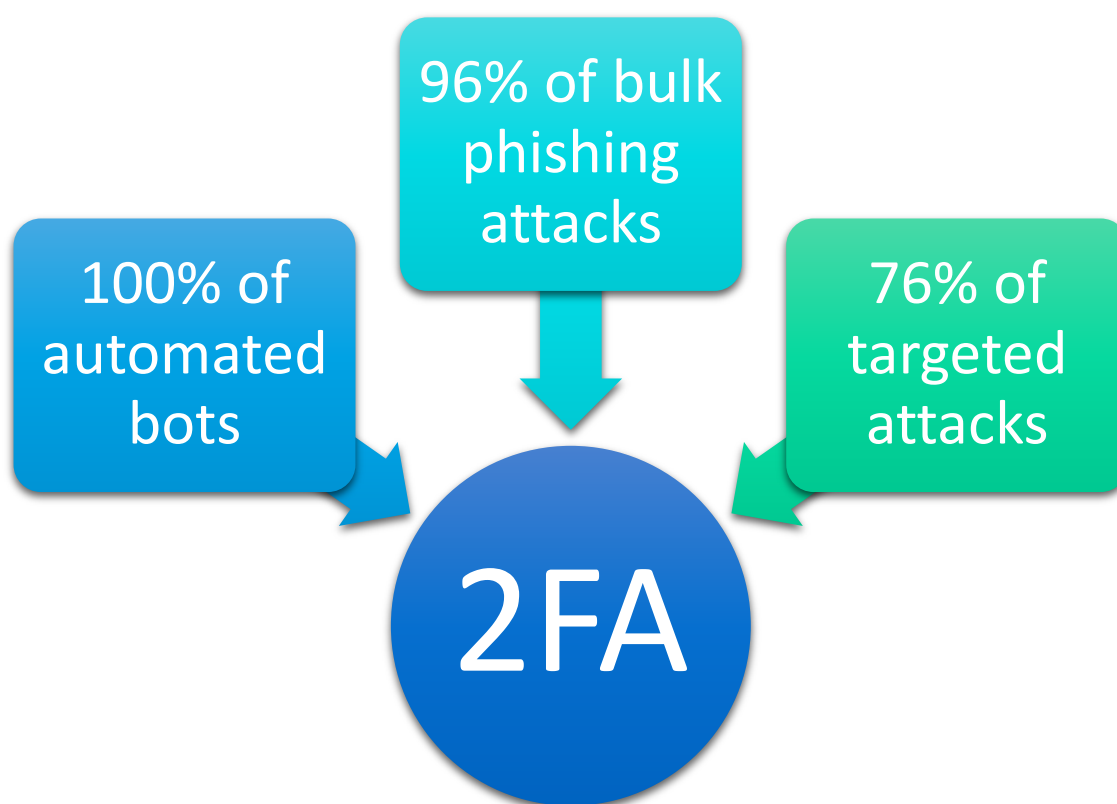


Figure 2 Percentages based on Google's 2019 2FA Report. Source: [Google Online Security Blog](#)

5. INSTALL ANTI-MALWARE SOFTWARE



The most prevalent method for combating malicious attacks has been anti-malware software. Antivirus typically deals with older, more established threats, whereas anti-malware focuses on newer threats. Anti-malware software also typically updates its definitions faster than antivirus software, making it the best defense against new malware you may encounter while surfing the web. Use trusted anti-malware software and only run one tool on your device. Most software will work alongside Windows' built-in Virus and Threat Protection. [Malwarebytes](#) is one of the most effective anti-malware applications available. They provide real-time malware and spyware protection, and their free version still surpasses many others. Malwarebytes is available on Windows, iOS, and Android, so everyone can benefit from their protection.

Time it Takes a Hacker to Brute Force Your Password in 2022					
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	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Figure 3 Time It Takes a Hacker to Brute Force Your Password in 2022. Data sourced from: [Hive Systems](#)

6. BE CAUTIOUS ABOUT WHAT YOU POST ONLINE

Most people are aware that they shouldn't share their social security number or credit card information online. However, there is a lot of other Personally Identifiable Information (PII) that people regularly share without thinking twice. PII is any data that could potentially identify a specific individual. This includes, but is not limited to, your full name, home address, date of birth, email address, and phone number. The amount of people that post their phone numbers and addresses on social media is surprising. Hackers can use this information to commit identity theft, or they may sell your information to other criminals.

You shouldn't assume that hackers are the only threat, either. While you may exercise caution when posting online, your loved ones may not. They might tag you in pictures or status updates without asking first. Keeping tabs on who sees and uses that data after it has been made public can be difficult.

The best way to protect your PII is to be cautious about what you share online. **Think about whether you really need to share a piece of information before you post it.** If you're not sure, it's probably best to err on the side of caution and keep it private. Otherwise, you could be the next victim of identity theft.

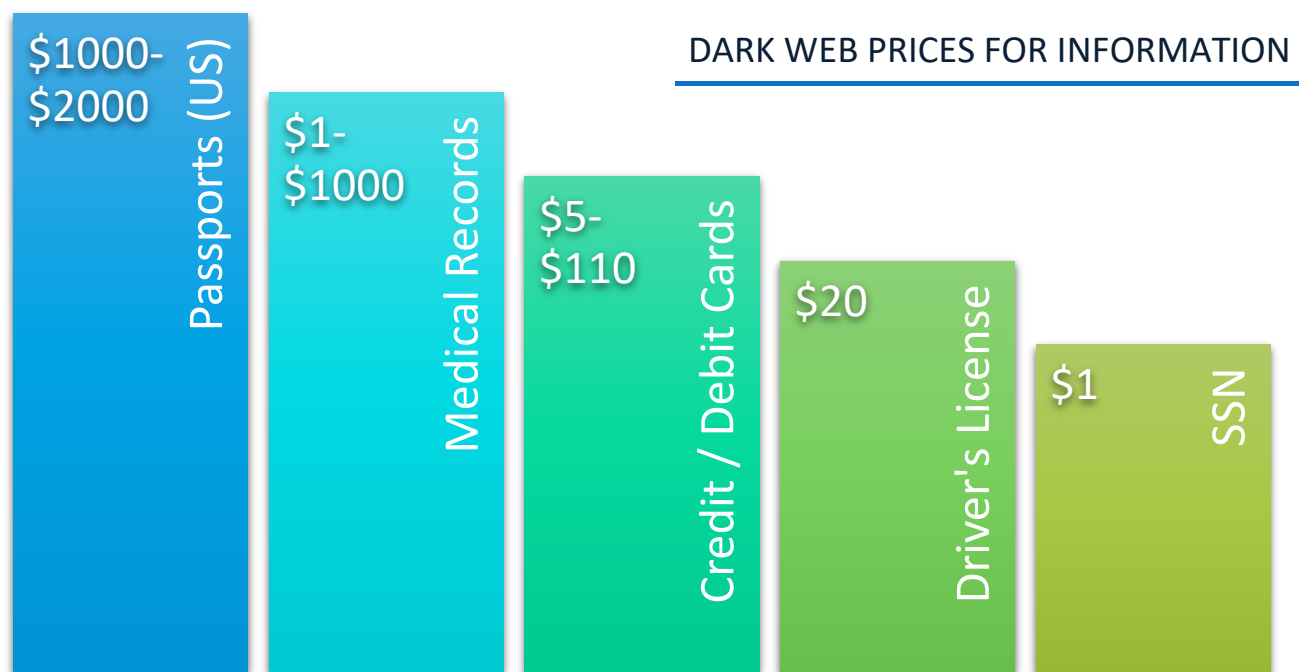
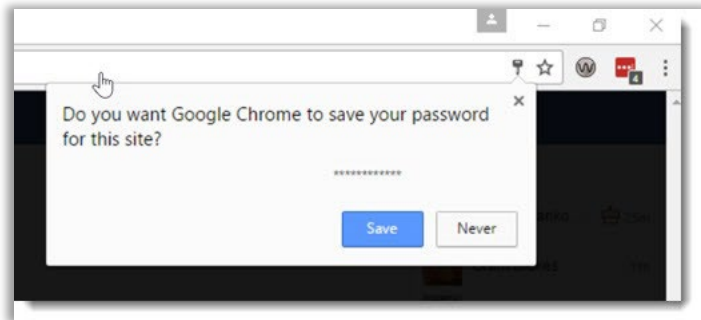


Figure 4 What the Most Common Pieces of Information Sell for on the Dark Web. Data Sourced from: [Experian](#)

7. DO NOT STORE PASSWORDS OR CREDIT CARDS

Storing your passwords, usernames, and credit card numbers on your computer may seem like the best way to remember them all, especially if you follow experts' advice and don't use the same passwords twice. **However, browsers store passwords in a list you can access at any time, which many viruses and malware can steal remotely.**



[This article](#) demonstrates how hackers can extract your passwords with just 12 lines of code. A password manager such as Bitwarden is an encrypted data vault that locks automatically when not in use, requiring hackers to breach it to gain access to your passwords.

Even if you do not save your passwords to your browser, storing credit card numbers when shopping online puts you at risk, too. If you frequently shop on Amazon or Walmart.com, saving your credit card information to speed up the checkout process may seem like a good idea. However, if the website suffers a data breach, your credit card information could be compromised. Experian has [an article](#) with safety tips. If you truly want to save your information, [Bitwarden](#) also allows you to save credit card numbers.



+93%

More than 93 percent of healthcare organizations experienced a data breach from 2017 to 2020.
([Herjavec Group](#))

233 days

Financial services businesses take an average of 233 days to detect and contain a data breach.
([Varonis](#))

45%

Personal data was involved in 45 percent of breaches in 2021.
([Verizon](#))

8. BE CAUTIOUS WITH PUBLIC WI-FI

Unsecured networks can be used by anyone to propagate malware and access sensitive information. One of the most dangerous aspects of free Wi-Fi is the ability of hackers to place themselves between you and the connection point. This is called a man-in-the-middle attack, and rather than communicating directly with the hotspot, you wind up transmitting your information to the hacker. This type of attack is particularly dangerous because the victims may not realize that they are being attacked, and the attacker can easily eavesdrop on or modify the communications between the two victims. They will also have access to all the information you send out, including emails, phone numbers, credit card information, and so on.



Figure 5 Risks of Public Wi-Fi. Source: [Norton](#)

Unfortunately, many public wi-fi networks are not secure. The simplest solution is to not use public Wi-Fi at all, but if you must, the best method you can use to protect yourself is to use a Virtual Private Network (VPN). By using VPN software, the traffic between your device and the VPN server is encrypted. This means it's much more difficult for a cybercriminal to obtain access to your data on your device. Use your cell network if you don't have one, but ProtonMail offers a [free VPN](#) when you sign up for the world's most secure (*and free!*) email. Additionally, it is important to be cautious when using public wi-fi and to avoid accessing sensitive information (such as banking information) while connected to a public network.

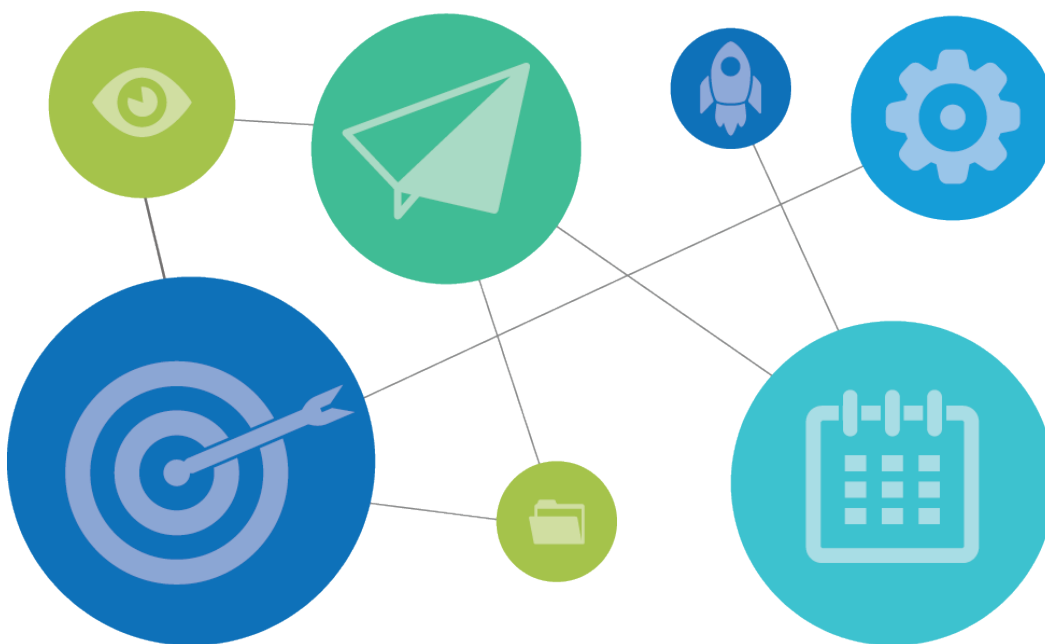
9. CREATE A SECURE EMAIL



Email is a critical part of our online lives. We use it to communicate with friends, family, and colleagues. We use it to sign up for websites and online services. And, most importantly, we use it to store and manage our personal information, like financial documents and medical records. That's why it's so important to have a secure email account. Your recovery, or alternate, email address is an additional email address you list in your security settings to use when you are unable to sign in normally or forget your password. A recovery email address should be on a different and more secure email service, such as [ProtonMail](#). ProtonMail is the world's largest secure email service. They offer end-to-end encryption and store your data in secure data centers located in Switzerland - a country with some of the strictest privacy laws. They ensure your communications are kept private - even they have no way of reading them. They also offer a [free VPN](#) for extra security should you want it.

if you're looking to protect your online information, be sure to create a secure recovery email account. It could be the difference between losing everything and regaining control of your online life.

THE WEAK LINK: Your level of digital security is only as strong as the level of your weakest recovery email account's security.



10. MONITOR YOUR CREDIT

With the surge in cyberattacks, it's more crucial than ever for people to protect their accounts and keep an eye on their credit reports. Right now, the most efficient strategy to safeguard your personal credit information from hackers is to implement a credit freeze. It essentially allows you to lock your credit and utilize a personal identification number (PIN) known only to you. You can then use this PIN when applying for credit.

credit karma

If a credit freeze is not something you can or are willing to do, you can still take steps to safeguard your identity. There are several websites that offer a free credit report. The only official government-supported website is annualcreditreport.com, but you can only view it for free once yearly from each of the credit bureaus. While this is still highly encouraged, you can also sign up for websites like creditkarma.com to access your information any time you want. They also send you credit alerts if anything important changes on your TransUnion credit report. This can help you spot identity theft and fraud. They also offer financial calculators and educational articles if you're interested.

2022 cybersecurity trends taking shape



- » A growing number of people around the world are using the internet, which means more people are falling prey to cybercriminals every year.
- » Cyber fatigue has gripped organizations whose teams have given up proactive defense.
- » Cybercriminals will continue to target remote workers.
- » The cybersecurity skills gap will worsen as more jobs go unfilled.

Source: [Varonis](#)



HOW TO REPORT A CYBERSECURITY INCIDENT

Most people don't think about cybersecurity until after they've been attacked. But everyone, not just businesses, needs to care about cybersecurity. Because of this, it's important for users to report any problems right away, no matter how small. If you've been the victim of a cyberattack, the first thing you should do is report it to the authorities.

In the US, you can report incidents to the FBI's Internet Crime Complaint Center (IC3). The IC3 is the best place to report if you're not sure where else to go. Additionally, CISA allows internal and external parties to report incidents, phishing attempts, malware, and vulnerabilities. You can submit a report online at <https://www.cisa.gov/report>. You can also report an incident to your local police department, but they may not have the resources to investigate a cybercrime. If you're a victim of identity theft, you should also file a report with the Federal Trade Commission.

If you don't report an incident, you may lose your right to a police report or insurance claim. On the other hand, reporting the incident may prevent others from becoming victims or help law enforcement apprehend the perpetrator. Here's what you need to know about reporting a cybersecurity incident.

1. First and foremost, don't panic. When you learn that your personal information has been compromised, it can be tempting to go into a frenzy, but it's crucial to maintain your composure and your ability to reason.
2. Step back and evaluate the situation. Determine how the incident occurred and what data might have been compromised.
3. Take steps to protect your account and prevent further damage. This may entail changing your passwords, updating your security settings, or even canceling your credit card if it was compromised.
4. Notify and contact the necessary parties directly. This includes your bank, credit card company, and any other affected businesses. If you've been a victim of a phishing attack, for example, you can report it to the company that was impersonated.
5. Make sure to document everything that took place, including any conversations you had with the attacker and any money you lost. This will be helpful if you need to file a police report or make an insurance claim. If you've been a victim of identity theft or another serious crime, you should always file a police report.

Reporting a cybersecurity incident can be overwhelming, but it's important to do it as soon as possible. By taking these steps, you can help protect yourself and others from future attacks.

HOW TO REPORT A CYBERSECURITY INCIDENT

Step 01

First and foremost, don't panic. When you learn that your personal information has been compromised, it can be tempting to go into a frenzy, but it's crucial to maintain your composure and your ability to reason.

Step 02

Step back and evaluate the situation. Determine how the incident occurred and what data might have been compromised.



Step 03

Take steps to protect your account and prevent further damage. This may entail changing your passwords, updating your security settings, or even canceling your credit card if it was compromised.

Step 04

Notify the necessary parties. This includes your bank, credit card company, and any other affected businesses or organizations. Contact the company or organization directly. If you've been a victim of a phishing attack, for example, you can report it to the company that was impersonated.

Step 05

Make sure to document everything that took place, including any conversations you had with the attacker and any money you lost. This will be helpful if you need to file a police report or make an insurance claim.



CYBERSECURITY RESOURCES

Software and Tools

- ☐ Free Password Manager - <https://bitwarden.com/>
- ☐ Free Anti-Malware - <https://www.malwarebytes.com/>
- ☐ Clear Your Privacy Trackers - <https://www.ccleaner.com/>
- ☐ Best Secure Email - <https://protonmail.com/>
- ☐ Free Secure VPN - <https://protonvpn.com/>
- ☐ Private Search Engine - <https://duckduckgo.com/>
- ☐ Free Credit Monitoring and Reports - <https://www.creditkarma.com/> | <https://www.annualcreditreport.com/>

Guidance and Good Practice

- ☐ Search for Yourself on A Data Breach Site - <https://haveibeenpwned.com/>
- ☐ Remove Your Info. from Public Search Engines - <https://the.osint.ninja/optoutdoc>
- ☐ How to Answer Security Questions Securely - <https://defendingdigital.com/how-to-answer-security-questions-securely/>
- ☐ Is It Safe to Store My Credit Card Information Online? - <https://www.experian.com/blogs/ask-experian/should-you-store-credit-card-information-online/>


Reporting

- ☐ CISA Incident Reporting Form - <https://www.cisa.gov/report>



REFERENCES

- [1] IBM, "Cost of a Data Breach 2022," [Online]. Available: <https://www.ibm.com/reports/data-breach>.
- [2] World Economic Forum, "Global Risks Report 2022," 11 January 2022. [Online]. Available: <https://www.weforum.org/reports/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities#chapter-3-digital-dependencies-and-cyber-vulnerabilities>.
- [3] R. Sobers, "64% of Americans Don't Know What to Do After a Data Breach - Do You?," 24 September 2021. [Online]. Available: <https://www.varonis.com/blog/data-breach-literacy-survey>.
- [4] World Economic Forum, "After reading, writing and arithmetic, the 4th 'R' of literacy is cyber-risk," 17 December 2020. [Online]. Available: <https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education>.
- [5] Verizon, "2022 Data Breach Investigations Report," [Online]. Available: <https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf>.
- [6] E. G., "Over 150,000 COVID-Related Fraud Reports Submitted to the US Government YTD," 4 August 2020. [Online]. Available: <https://atlasvpn.com/blog/over-150-000-covid-related-fraud-reports-submitted-to-the-us-government-ytd>.
- [7] C. Brooks, "More Alarming Cybersecurity Stats for 2021!," 25 October 2021. [Online]. Available: <https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021->.
- [8] III, "Facts + statistics: Identity theft and cybercrime," [Online]. Available: <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>.
- [9] NordPass, "Top 200 Most Common Password List 2021," 2021. [Online]. Available: <https://nordpass.com/most-common-passwords-list/>.

- 
- [10] C. Neskey, "Are your passwords in the green?," 02 March 2022. [Online]. Available: <https://www.hivesystems.io/password>.
- [11] K. Thomas and A. Moscicki, "New research: How effective is basic account hygiene at preventing hijacking," 17 May 2019. [Online]. Available: <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>.
- [12] T. Seals-Dormer, "One simple action you can take to prevent 99.9 percent of attacks on your accounts," 29 January 2021. [Online]. Available: <https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>.
- [13] E. Hasson, "Bad bot report 2021: The pandemic of the internet: Imperva," 13 April 2021. [Online]. Available: <https://www.imperva.com/blog/bad-bot-report-2021-the-pandemic-of-the-internet/>.