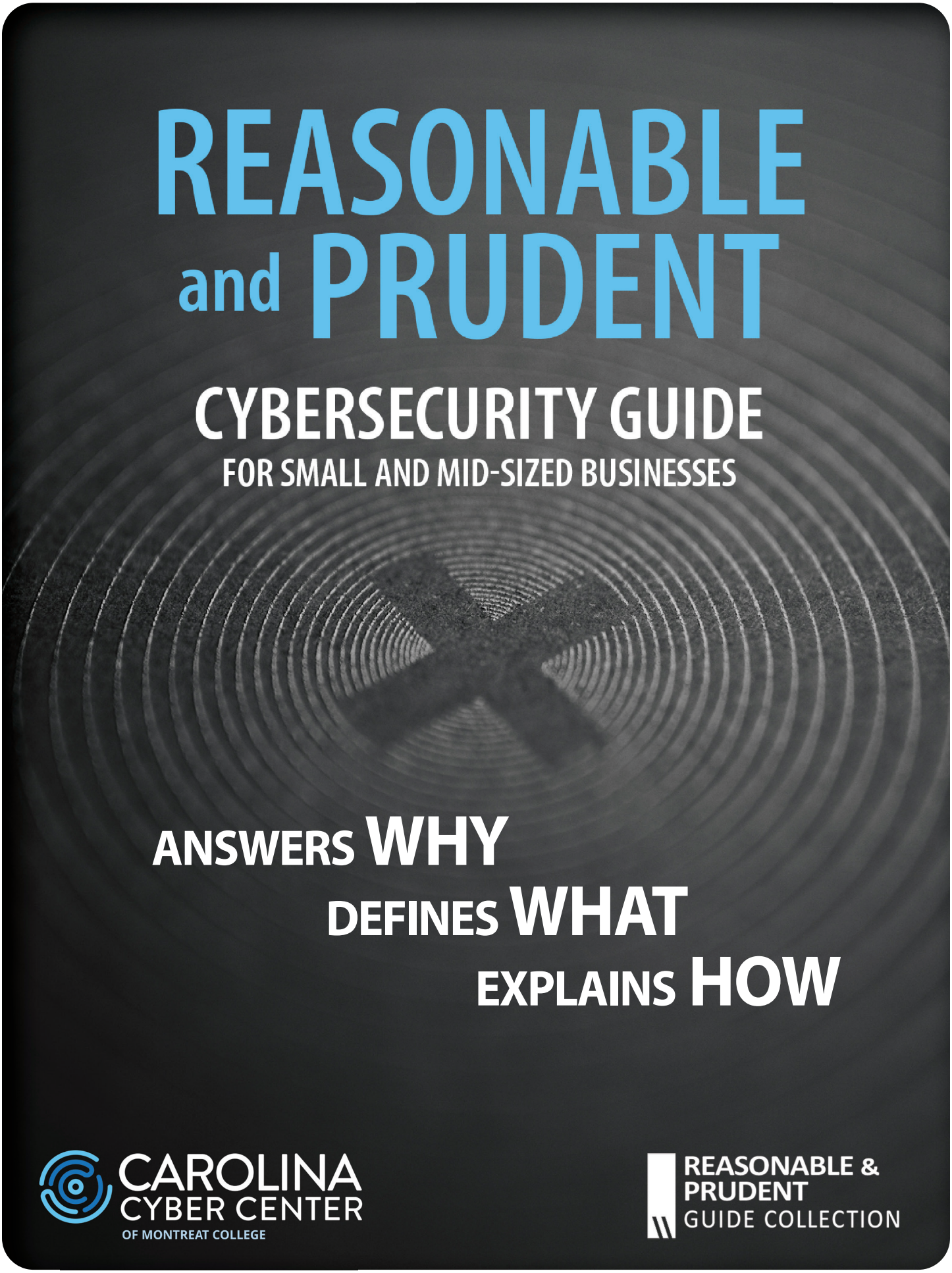
REASONABLE and PRUDENT

CYBERSECURITY GUIDE

FOR SMALL AND MID-SIZED BUSINESSES



ANSWERS **WHY**

DEFINES **WHAT**

EXPLAINS **HOW**

CAROLINA CYBER CENTER
OF MONTREAT COLLEGE

REASONABLE & PRUDENT
GUIDE COLLECTION

Title page

TABLE OF CONTENTS

Why Another Guide to SMB Cybersecurity? 5

How Bad Is Cybercrime in America… and WNC? 5

And, What is "Reasonable and Prudent" Anyway? 6

Key Words 7

How To Use This Guide 8

Measure 1: User Hygiene 101 9

Step 1: Multi-Factor Authentication 9

Step 2: Password Setting and Management 11

Step 3: Secure Browsing 12

Step 4: Social Engineering & Awareness Training 12

Step 5: VPN's 13

Measure 2: Network Hygiene 101 14

Step 1: Asset Discovery & Definition 14

Step 2: Asset Management - Patching 15

Step 3: Vulnerability Assessment & Remediation 15

Step 4: Basic Endpoint Hardening 16

Measure 3: Conduct a Proper Risk Assessment X

Step 1: Baseline Assessment X

Step 2: Maturing Your Cybersecurity Plan (POAM) X

Measure 4: Administration Basics X

Step 1: Define Key Basics X

Step 2: Ensure Employees Awareness & Accountability X

Measure 5: It's Not If, but When X

Step 1: Craft Your Incident Response (IR) Plan X

Step 2: Conduct Fun Tabletop Exercises X

Measure 6: Technical Staff Training X

Step 1: Basics of Cybersecurity X

Step 2: Top 11 Resilient Measures X

Step 3: It's All About the End User X

Measure 7: Secure Email (in and out) X

Step 1: Basics of Securing Microsoft 365 X

Step 2: Set up: DMARC/DKIM/SPF X

Step 3: Email Gateway X

Step 4: Other Email Protections X

Measure 8: Network Hygiene 201 X

Step 1: Credentials Management X

Step 2: Proper Logging / Auditing & Review X

Step 3: Port Mirroring (Network Monitoring & DNS) X

Step 4: Firewalls: Segmentation X

Step 5: Application Allow Listing X

Measure 9: User Hygiene 201 X

Step 1: Harden End User Devices X

Step 2: Active Directory Hardening X

Step 3: Personal Hygiene vs. The Office X

Step 4: Cyber Escape Room Exercise X

Measure 10: Detection X

Step 1: Setup Honey Docs X

Step 2: Setup Honey Accounts X

Step 3: Deploy IDS/EDR X

Measure 11: Transferring Risk with the Right Partners X

Step 1: MSP (e.g., RACI for internal vs. external IT) X

Step 2: MSSP (vs. MDR) (and the difference) X

Step 3: vCISO X

Step 4: Attorney and Contracts X

Step 5: Selecting Cyber Insurance Insurance: Scope & Provider (and why) X

Step 6: Retainers and Using IR Firms X

Measure 12: Now, Implement Key Routines X

Step 1: Save you from the "poverty of your intentions" X

What's Your Score (and near-term priorities)? X

How You Can Help X

Sources of Information and Inspiration X

Why Another Guide to SMB Cybersecurity?

There are many guides to cybersecurity, and many are pretty good! However, most guides have one or more key deficiencies:

1. Tell you ***what*** to do, but not clearly ***why*** (and this motivation wanes).
2. Were developed by a vendor trying to sell you something.
3. Don't give you a roadmap with straightforward instructions on ***how*** to do it.

We have produced a guide that:

1. Respects your time – *gets to the point!*
2. Defends why these measures substantially improve your cybersecurity.
3. Uses everyday language - not industry jargon.
4. Enables you to measure progress (much like a "cyber credit score.")

The Carolina Cyber Center support team is here to help! Our mission is:

Develop cybersecurity professionals of character while delivering services to measurably improve the security and resilience of regional public and private resources.

Thus, our goal is to "measurably improve the security and resilience" of ***your*** business.

How Bad Is Cybercrime in America… and WNC?

This guide was written with you, the small/medium business (SMB) leader, in mind. Therefore, we get straight to the point:

- Cybercrime is bad. Really bad… and it's getting worse. 966% worse in just one year.
- The average cost of a cyberattack on a small business is over $25K[1].
- Only 10% of cybercrime is even reported[2].
- It's not if, but when. Over 50% of SMBs reported a cyberattack in 2020[3].

The security measures in this guide reduce cybercrime at least 90%.

[1] https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf (Page 25).
[2] https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf
[3] https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

Just as we went to press, a new analysis of cyberattack data by security vendor Fortinet[4] sheds light on the volume of ransomware and who's being attacked the most.

- The weekly average number of ransomware attacks detected in June of 2021 was over 149,000. A year prior, it was only 14,000 – an increase of 966%[5]

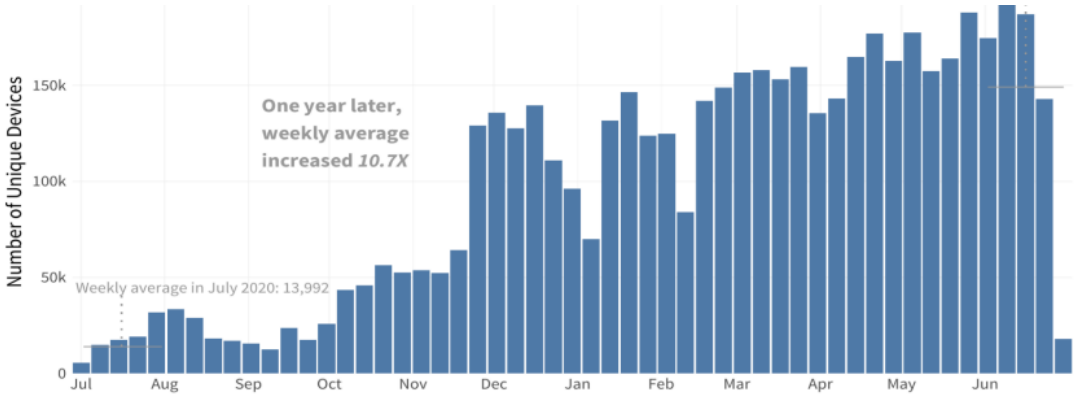


Figure 9: Growth in ransomware detections over last 12 months (Jul '20 - Jun '21).

- Over one-third of businesses in the Automotive, MSSP, Government and Telecom industries and one-quarter of nearly all other sectors experienced ransomware attacks.[6]

What is "Reasonable and Prudent" in Cybersecurity Anyway?

After interviewing over one hundred business leaders in WNC we came to understand the need for this "Reasonable and Prudent Guide to Cybersecurity for SMBs." Specifically, a guide that lays out reasonable steps – steps for which it is *reasonable* to expect that you or your IT lead (inhouse or managed IT service provider) can do with existing skills and abilities. They just need time and (in some cases) a little money. We also focus only on the *prudent* measures – measures clearly able to address the most common threats.

We developed this guide to adhere to our state motto *esse quam videri* (to be rather than just to seem). Nothing difficult, just practical advice with clear steps to make the biggest improvements as fast as possible.

As we endeavor to serve our community, we look forward to your counsel on how we can be of more service and improve future editions of this guide.

Warm regards,

Adam C. Bricker
Executive Director, Carolina Cyber Center
Adam.Bricker@CarolinaCyberCenter.com
(828) 419-2311 x3511

[4] https://www.sbir.gov/tutorials/cyber-security/tutorial-1#
[5] https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-2021-threat%20landscape.pdf
[6] https://blog.knowbe4.com/the-number-of-daily-ransomware-attacks-increase-nearly-1000-in-2021

Key Terms

The following terms are used throughout this document.

Risk – The probability of exposure, loss of critical assets and sensitive information multiplied by the magnitude of the exposure.

Cybersecurity – We prefer the terms “Data Care” and “Information Security,” but since most people use the term “Cybersecurity” we use that as well. The definition we use is: Cybersecurity is managing risk of unauthorized disclosure, modification, and destruction of information using organizational, physical and technical controls. To be clear, Cybersecurity is a business risk, not just an “IT matter.”

Cyber Resilience – An entity's ability to continuously deliver the intended outcome, despite adverse cyber events.

Risk Transfer – A risk management and control strategy that involves the contractual shifting of a pure risk from one party to another.

Vulnerability – A weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries within a computer system.

Threat – A potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.

Phishing – The fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.

Plan of Action and Milestones (POAM) – A plan that describes specific measures to be taken to correct deficiencies found during a security control assessment.

How To Use This Guide

Follow the steps!

Resilience points are defined to help you measure progress on your Information Security journey. By following the simple steps in this guide, you "earn" resilience points associated with each measure and step. You will also be able to compare yourself with other businesses like you. Add your points for each completed step to evaluate your cyber maturity for a resiliency score (e.g., 62 out of 100 points is a score of 62% **resiliency**). For reference, the total score for this guide, the first of several guides to come, is out of 100 points. The Carolina Cyber Center is producing a series of "Reasonable and Prudent" guides, but let's get through the basics first!

Know you are not alone!

At the Carolina Cyber Center Business Luncheon, we gave you the first step to having a more secure environment. This guide introduces twelve measures we hope you will take over the coming weeks or months. An advocate was assigned to you and your group at the September 22, 2021, luncheon. This advocate will check in and support you during your journey thru the 12 measures.

Understand that cybersecurity standards evolve rapidly.

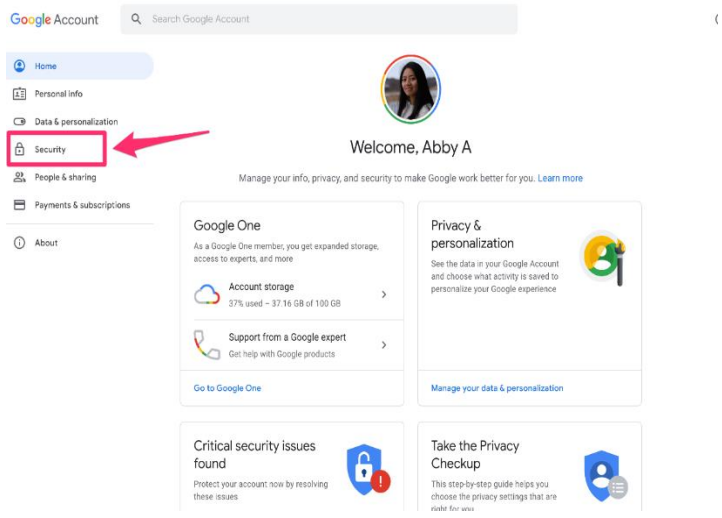
The Information Security work is never truly finished, which is why we train, compete, and journey together. We will continually update this guide to reflect changes in threats, defense tactics and solutions. If you have made it to this page, you've shown the intent to improve your posture and security score! Press on for the first step in that journey…

Measure 1: User Hygiene 101

Step 1: Multi-Factor Authentication (+10 Resiliency Points)

Skill Level: Self or IT Admin; Cost: Free; Time: 1.5 Hours

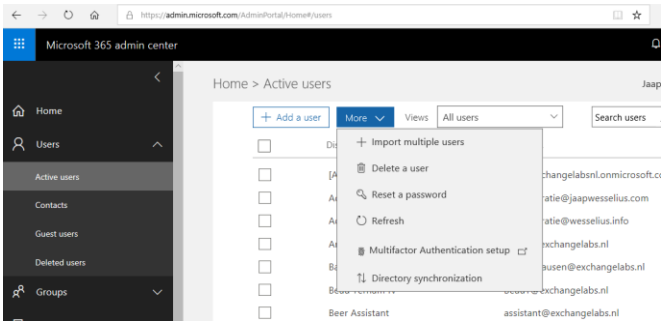
- **What:** When you sign into an account it is called 'authentication.' Commonly, this is done with a username and password. Since usernames and passwords are too easy to crack, many services have offered a way for your accounts to be more secure. *Multi-factor authentication (MFA)* is using multiple forms of authentication via something you know (password or pin), something you are (fingerprint or biometrics), and something you have (text to your mobile phone, smart cards, security tokens). This is sometimes referred to as *Two-factor authentication* when it requires two out of the three types of authentications such as a password and a code sent to your smart phone.
- **Why:** Multi-factor authentication is like your house. You most likely do not have a single lock to your front door. Instead, you have a lock on your handle and a deadbolt. Some people even have a door latch as well. It is the same concept with your cybersecurity and protecting your business' data. You want as many locks as possible to deter the attackers or bad guys. Microsoft says that *MFA can block over 99.9 percent of account compromise attacks.* With MFA, knowing or cracking the password won't be enough to gain access.[7]
- **How:** First, enable this for your personal and business email. This is the most likely point of entry for an attacker, as is your front door to an intruder. Next, it is important that this is done for any cloud service such as your machine/hosts, active directory, ERP/HR, Accounting tools, bank accounts, just as you would lock your windows, back doors, etc. Below are the steps for the major email account types (the others are similar):
- Gmail:
    1. Open your Google Account with global admin credentials.
    2. In the navigation panel, select Security.
    3. Under "Signing into Google," select "2-Step Verification- Get Started"
    4. Follow the on-screen steps.[8]



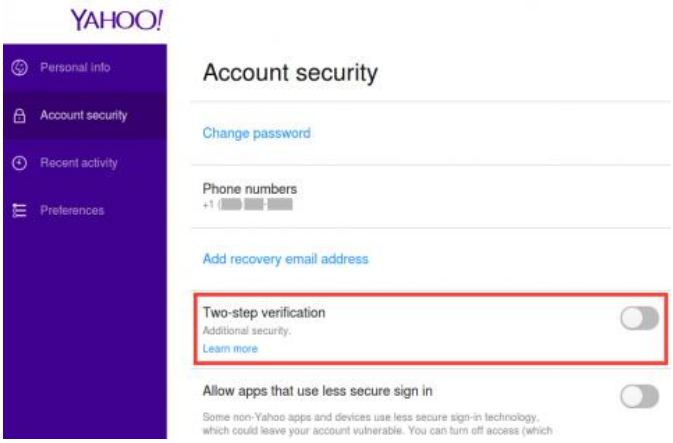
[7] https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

[8] https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3DDesktop

- Outlook:
    - Note: If you purchased your subscription or trial after October 21, 2019, and you're prompted for MFA when you sign in, security defaults have been automatically enabled for your subscription.
    1. Sign into the Microsoft 365 admin center with global admin credentials.
    2. In the left navigation panel choose Show All and under Admin centers, choose "Azure Active Directory."
    3. In the Azure Active Directory admin center choose "Azure Active Directory > Properties."
    4. At the bottom of the page, choose "Manage Security Defaults."



    5. Choose "Yes" to enable security defaults or "No" to disable security defaults, and then choose "Save."[9]
    6. The next time you and your employees log in, you will be prompted to set up authentication via your phone.
- Yahoo:
    1. Mouse over your name in the upper right-hand corner and click "Account Info."
    2. On the left-hand bar, choose "Account security." Move the toggle by "Two-step verification" to the right to start set-up.
    3. Enter your mobile phone number. You'll need to be able to receive text messages and/or voice calls at this number. Click the one you'd prefer.
    4. Soon after you click, you should receive a text or call with your code. Enter the code and click "Verify."



    5. With set-up complete, you'll have the option to generate third-party app passwords—that is, passwords for devices and applications that do not support logging in using a one-time verification code. You'll want to generate app passwords if you access your Yahoo Mail account on other platforms like iOS Mail, Android Mail, or Outlook.[10]

[9] https://support.microsoft.com/en-us/office/set-up-your-microsoft-365-sign-in-for-multi-factor-authentication-ace1d096-61e5-449b-a875-58eb3d74de14
[10] https://www.eff.org/deeplinks/2016/12/how-enable-two-factor-authentication-yahoo-mail

Step 2: Password Setting and Management (+10 Resiliency Points)

Skill Level: Self or IT Admin; Cost: Free, up to $8 per user/per month; Time: 1 Hour

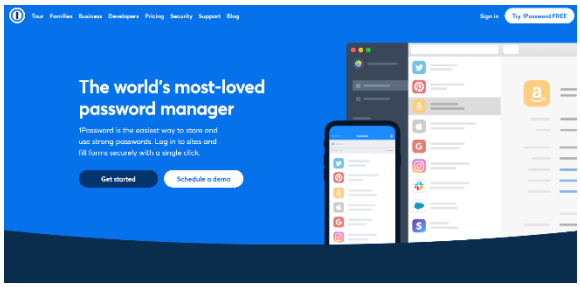
What: Here's what's important about passwords: using unique, strong passwords for each website/system, and keeping those passwords private. Passwords should be *at least* 14 characters and complex (made up of special characters, numbers, and letters). Password managers generate passwords for you based on the settings that you provide.

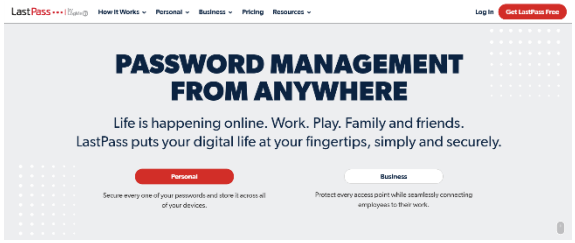
Why: Password managers create, store, and use (auto-populate) complex passwords. These tools can also secure other private data such as your email addresses, usernames, and credit card information.

How: These are two of the industry's top password managers. They will generate passwords for you and can be added as browser extensions.

Below are the steps for setting up the password managers:

- 1Password
    1. Sign up on 1password.com
    2. Get the apps on all your devices (e.g., computer, phone, iPad)
    3. Save, fill, and change all your passwords
- LastPass
    1. Sign up on lastpass.com
    2. Get the apps on all your devices (computer, mobile phone, iPad, etc.)
    3. Save, fill, and change all your passwords





Step 3: Secure Browsing and Search (+2 Resiliency Points)

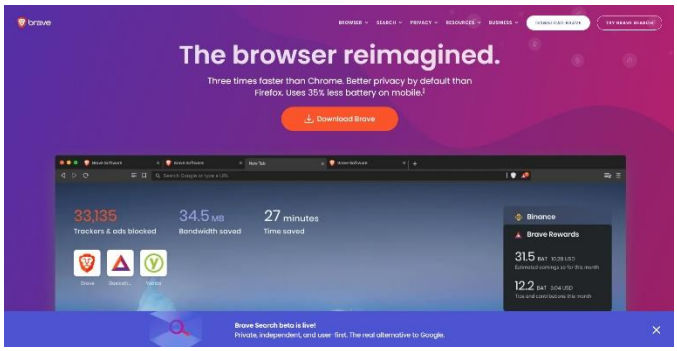
Skill Level: Self or IT Admin; Cost: Free; Time: 1 Hour

What: Secure browsers are ones that protect your privacy by using ad blockers, browser fingerprinting protection and its privacy focused nature. Brave is a chromium-based browser that blocks ads, blocks scripts, blocks third party storage and automatically upgrades all connections to HTTPS. Secure search engines help protect you from having your private data and search history tracked and collected.

Why: A secure browser that protects your privacy is a critical tool for staying safe online and keeping your data secure from third parties. In this guide we are going to be analyzing the most secure browsers that also respect your privacy. Third party companies attempt to collect browsing history, login credentials, cookies and trackers, and auto fill information. Secure

browsers like Brave and secure search engines like DuckDuckGo protect your privacy against all of these.

How: Below are the steps to set up Brave and DuckDuckGo (there are other good platforms out there, just a couple of examples…).



How to set up a secure browser such as Brave:

1. Go to Brave.com
2. Download Brave
3. Go to machine settings > Default Browser > select Brave > Save

How to set up a secure search engine like DuckDuckGo:

1. Go to https://duckduckgo.com/install
2. Right click in the search bar
3. Select 'Edit Search Engines' in the dropdown
4. Find DuckDuckGo and click "Make default"
5. Install and use on mobile devices as well

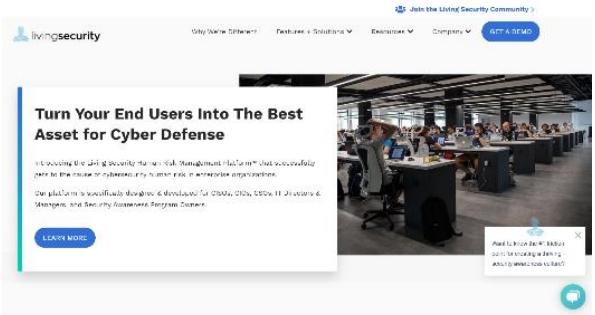
Step 4: Social Engineering & Awareness Training (+2 Resiliency Points)

Skill Level: Self or IT Admin; Cost: Free, up to $10 per user/per month; Time: 5 Hours to set up

What: Training that teaches the end user (any employee) how to act and defend against attacks is called end user awareness training. This can be done in a multitude of ways. Most common are videos, quizzes, and exercises. The most effective type of cyber defense for end user training is a combination of videos and exercises, but additionally, testing employee's knowledge.

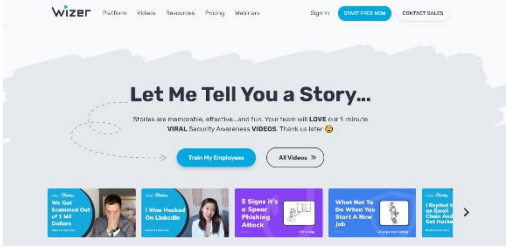
Why: Everyone is taught what to do in a fire drill. And we're taught what to do if our clothes catch on fire: stop, drop, and roll. These steps come second nature to us. This is how it should be for cybersecurity incidents. Users should be trained to know when someone is trying to social engineer them to give up company information, just as one should know how to calmly exit the building when the fire alarm goes off.

How: Companies such as Living Security and Wizer have different ways that end users can be taught (sample at right). They both include interactive videos and exercises to help employees practice. Explore their options and decide which best fits your organization.



Links to the company's websites:

- Living Security: https://www.livingsecurity.com/
- Wizer: https://www.wizer-training.com/



Step 5: VPN's (+2 Resiliency Points)

Skill Level: Self or IT Admin; Cost: Free, but enterprise model pricing varies; Time: 2 Hours

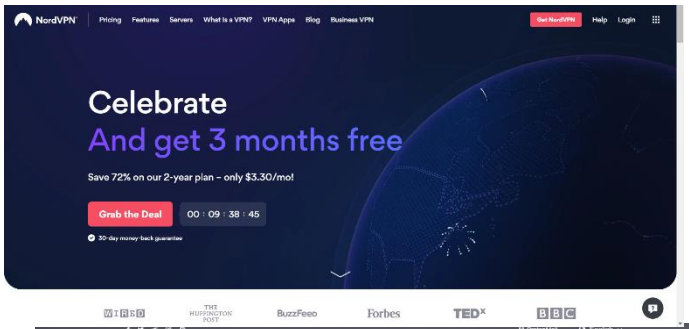
What: A Virtual Private Network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address, so your online actions are virtually untraceable. VPNs are used to establish a secure connection between you and the internet. VPNs protect your data and privacy online and should be used when you are connecting to public Wi-Fi hotspots.

Why: VPNs focus on data integrity and security when working remotely. VPN's use what is called a tunnel which prevents unauthorized people from eavesdropping on what you are doing on your computer. VPNs keep important documents confidential and safe and make sure you are the only one seeing your computer screen.

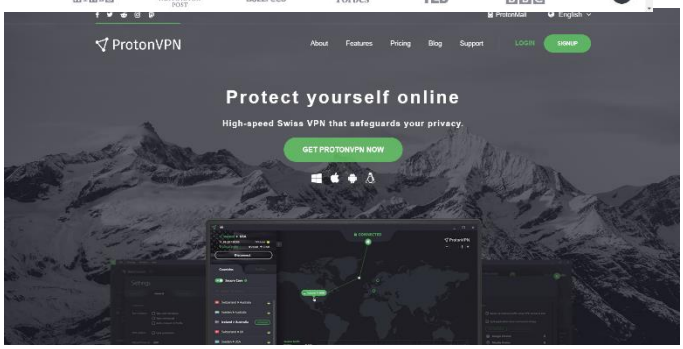
How: VPNs use a powerful form of encryption to keep you safe while surfing the web or working remotely. When using a VPN, your IP address is disguised, and you are virtually invisible to other users on the internet.

Below are the steps to set up a VPN for a couple of top vendors (again, the others are similar):

- NordVPN
  1. Go to nordvpn.com
  2. Select "GetNordVPN"
  3. Choose a plan
  4. Click "Quick Connect"
  5. Get the apps on all your devices (computer, mobile phone, iPad, etc.)



- Proton VPN
  1. Go to protonvpn.com
  2. Select "Signup"
  3. Choose a plan
  4. Click Connect
  5. Get the apps on all your devices (computer, mobile phone, iPad, etc.)
  6. Click "Connect"



Measure 2: Network Hygiene 101

Step 1: Asset Discovery & Definition (+5 Resiliency Points)

Skill Level: Self or IT Admin; Cost: Free; Time: 5 Hours

What: Asset management is obtaining and continually updating inventory of all devices on your network with a central processing unit (CPU), discovering security gaps that are related to the asset's configurations, and enforcing security requirements that address the gaps[11]. Assets can also include your data (that is why we want to protect it), hardware or software, or even your employees!

Why: The only way you can begin to address a problem is to first know you have one (a problem). Thus, in cybersecurity you need to know your assets and what your company has before you can determine if you have a problem.

How: There are many ways to catalog your assets, but the common ones are through some sort of systems management tooling, endpoint security software, vulnerability scans, or through cloud technologies. These subjects covered in more detail in future additions to our *Reasonable and Produce Guide* series.

Step 2: Asset Management – Patching (+10 Resiliency Points)

Skill Level: IT Admin; Cost: Free; Time: 5 Hours

What: Patching is updating the software to the latest hardened (most secure) version released. This can be done by an IT administrator, or it can be done automatically. Patches come from the vendor of the software/hardware product you are updating such as Microsoft, Apple, or Palo Alto.

Why: Patches are fixes or solutions to known problems. These problems or exploits are not only known by you, but also the attackers (bad guys). Thus, it is important to apply the patches/updates right away when they are released to ensure that you do not fall victim. It is like knowing that your pipes are leaking from the faucet. When you see water coming out of the pipe and onto your floor, you do not want to wait three days to call a plumber. Instead, you know that you need to act quickly because there is a problem.

How: The best way to patch your systems is to follow the steps listed below[12]:

1. Know your assets (do Step 1 above!)
2. Plan to standardize the version type (e.g., operating system, such as iOS) across machines
3. Keep your systems up to date (e.g., latest versions of Android, iOS, Microsoft – after you've confirmed these updates are compatible with critical systems – compatibility problems are rare, but keep an open mind)

[11] Gathering data from automated tools to discover and define details about each asset, setting a security policy for each asset and triggering actions whenever an asset deviates from the policy.

[12] https://www.rapid7.com/fundamentals/patch-management/

4. Make a list of the security controls that you have in place at your organization (firewalls, antivirus, vulnerability management tool, etc.)
5. Compare the vulnerabilities identified by the tool(s) (e.g., Nessus, Qualys, OpenVAS) against your inventory.
6. Determine which vulnerabilities you are susceptible too! Don't waste your time on ones that do not apply!
7. Determine the risk! Prioritize which assets need to be patched first.
8. Test out the patches on a sample of assets in a lab to ensure that they will not cause issues in your production environment.
9. Apply the patches.
10. Track the progress.

Step 3: Vulnerability Assessment & Remediation (+5 Resiliency Points)

Skill Level: IT Admin; Cost: Free, but enterprise tooling prices vary; Time: 10 Hours

What: A vulnerability is an opening or gap that could be exploited by an attacker. A vulnerability assessment is the process of defining, identifying, classifying, and prioritizing vulnerabilities in all your systems, applications, and networks.[13] The goal of an assessment is to provide the visibility to the risks that exist, and that external threats or the bad guys could take advantage of.

Why: Every organization faces the risk of cyber-attacks, and as we stated above, once you know the assets that your company uses, you want to protect them. When you first take driver's education, you are taught to inspect the car that you are driving before getting into it. That way you know if there is something that does not work, such as your headlights. It's the same concept here. You should want to 'inspect' your assets (or car) every time you use them. Fortunately, this can be readily automated. Now, this does not need to be done every single day, but it should be done on a regular basis, such as once a quarter.

How: There are many tools such as Qualys or Nessus that will do these scans for you, but ultimately it comes down to four basic steps[14]:

1. Initial Assessment – The goal is to understand the importance of devices on your network and the risk that each brings. Risk can be whether or not it has access to the internet (does it have an internal or external IP address), if the device is publicly accessible to anyone (such as a kiosk machine), whether a device's users have low-level or elevated privileges (such as administrators), or what is the device's role in the business process.

2. Define a system baseline - For each given device to be assessed for vulnerabilities, it's necessary to understand whether its configuration meets basic security best practices (ex: is it up to the most secure version?). Some of the configuration factors that should be a part of a baseline include:

    a. Operating system (OS), version, and service pack or build, if applicable

[13] https://cybersecurity.att.com/blogs/security-essentials/vulnerability-assessment-explained
[14] https://cybersecurity.att.com/blogs/security-essentials/vulnerability-assessment-explained

b. Approved software
c. Installed services and required ports
d. Any unnecessary open ports – ports that should be closed!
e. Any special security configuration, if applicable

3. Perform a vulnerability scan - In general, vulnerability scans are performed either via *unauthenticated* or *authenticated* methods. In an *unauthenticated* scan, a system is assessed from the network perimeter (as if an attacker was trying to test all your doors, windows, and locks to get into your house), looking for open ports, and testing for known exploits and attacks. An *authenticated* scan will perform a credentialed (i.e., using the ID and password to knowingly access the system) scan of the operating system and applications looking for misconfigurations and missing patches that can be taken advantage of by attackers, such as weak passwords, application vulnerabilities and malware (the bad guy is seeing if you are trained in martial arts or not).
4. Create a vulnerability assessment report – Creating a report that shows the results of the scan, the risk of the devices and the next steps is crucial. This is your playbook to create the overall game plan of how to make your business more secure. A sample vulnerability report, policy and other templates can be found at https://frsecure.com/resources

Step 4: Basic Endpoint Hardening (+3 Resiliency Points)

Skill Level: IT Admin; Cost: Free; Time: 3 Hours

What: Endpoint hardening is the concept of making your laptops, computers, servers, and other assets with a CPU hard to break into. Just as you add multiple locks and maybe a fence around your house, you also want the same security around each device.

Why: We all have heard the story about two hikers who see a bear and one turns to tie his shoe to run away and his friend says, "you'll never outrun a bear." The first hiker yells back as he is running away, "I don't have to, I just need to outrun you." This same story is echoed in cybersecurity. The bulk of cybersecurity attacks are not that sophisticated, and you want to be harder to break into then your 'next door neighbor' (other businesses like yours). That way the attacker will choose to attack them and not you, it is basic survival skills.

How: It really isn't much more then these measures and steps you have taken already. Now it is time to put them all together! [15]

1. Patch everything, faster – Aim to have full patch coverage within 48 hours of updates released by the respective vendors (Good thing you already completed this is Measure 2 step 2!).
2. Actively protect your devices – for example, enable Microsoft Defender for Endpoint on all your Windows machines. This is an easy-to-implement line of defense!

[15] https://www.microsoft.com/security/blog/2021/08/11/7-ways-to-harden-your-environment-against-compromise/

3. Reduce your exposure – Ensure all your devices are behind a firewall that restricts access[16]. This paired with multi-factor authentication (Measure 1 step 1) will dramatically help!
4. Reduce your privilege - Most attacks rely on the attacker obtaining administrative access. If we can limit exposure, we go a long way to blocking many attacks. Having a common local admin password makes lateral movement and elevation of privilege a trivial task for attackers. Local Administrator Password Solution (LAPS), which manages local administration accounts on systems, has been available for nearly six years and is free. Nonetheless, on many engagements, we see it has not been deployed. Deploy LAPS on your network today.
5. Pay down your technical debt - Running legacy (older versions) operating systems increases your vulnerability to attacks that exploit long-standing vulnerabilities. Where possible, look to decommission or upgrade legacy Windows, Linux, iOS and other operating systems.

Congratulations for completing Measures 1 and 2. You have already completed the most important steps (you know we would put these in order, right?) you can take to reduce your risks of cyberattacks – and reduce the cost of your cyber insurance, which we cover later.

Reach out to us at the Carolina Cyber Center (www.carolinacybercenter.com/contact or info@carolinacybercenter.com) to receive the next Measures and updates to this "living" guide to your cybersecurity.

Oh, and please let us know how we can improve this guide and serve you better!

[16] Disable ports and protocols not being used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389). Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts. Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the following actions to protect their networks: Disable SMBv1 and v2 and upgrade to SMBv3 (or most current version) along with SMB signing. Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139

Reasonable and Prudent Personal Cybersecurity Measures

The Carolina Cyber Center is committed to helping you secure your applications, data, and systems. So, we've created this guide to help you improve your "personal cyber hygiene." Note that most of these measures make your computer easier to use AND more secure! And all without costing you a penny!

We've also provided a scoring system so you can measure your cyber hygiene as it improves. As you move through the topics, add up your points to see how well you score at the end.
Here are the categories:

Reasonable and Prudent Personal Cybersecurity Measures 1

- Passwords 1
- Multi-Factor Authentication 5
- Virtual Private Network (VPN) 7
- Secure Web Browsing 10
- Secure Communications 10
- Securing Your Credit 12
- Data Protection - Backup 12

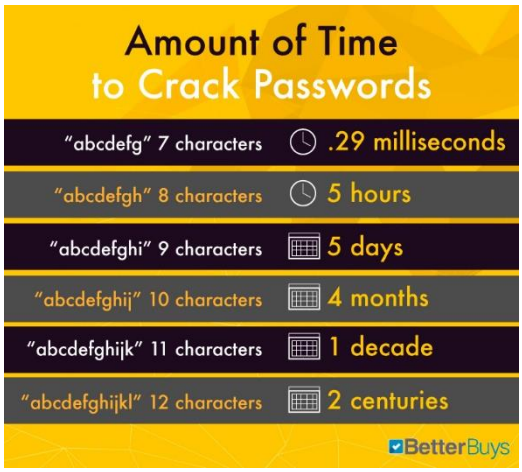
Total Score 13

Passwords

Here's what's important about passwords: using unique passwords for each website/system, choosing strong passwords, and keeping those passwords private. Therefore:

1. **(3 Points)** Don't use the same password on more than one system. Because if that one password gets cracked, the bad guys can access every one of your other systems that use the same password. Also, use longer, "phrase-based" passwords instead of shorter, "word-based" passwords. For example, *CatsandDogsRunCrazy!* is easier to remember and harder for the bad guys to crack than *$3fgT67*. And if the idea of creating unique passwords that are long and complex worries you, just keep reading! We will introduce you to password managers below. Password managers are tools that create and store long and complex passwords you don't have to remember.

2. The combination of your username and password is a form of computer "credentials". Password managers securely store your credentials and make it simple to use long passwords. Why are long passwords so important? Well, see the table at the right – which is WRONG. Many malicious actors now have "rainbow tables" that enable them to crack most passwords up to 12 characters. Thus, chose a password of AT LEAST 14 characters if the system will permit

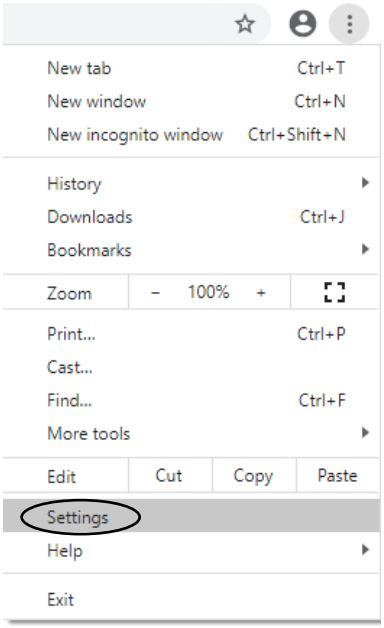


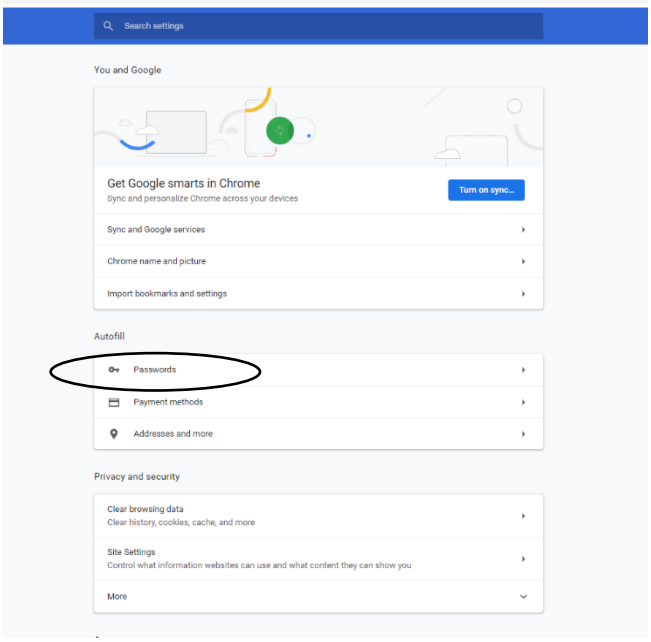
   Fortunately, password managers usually auto-detect the site you are browsing and auto-populate your credentials in the correct fields – so it does not take any more time to enter an 8 character versus a 15 character password.

(3 Points) Therefore, install and use a password manager (e.g., 1Password, LastPass) to make it easy to create, store, and use complex passwords. These tools can also secure other private data, such as your email address or your credit card info. Do NOT ***ever*** use the password and credential form-filling features from your browser (e.g., Chrome). And don't store your credit card information in your browser, either. Go ahead and erase your browser-based passwords/credentials (e.g., in Firefox, Chrome, Edge). Then use a password manager to automate making all your passwords unique, and you won't have to remember them anymore!

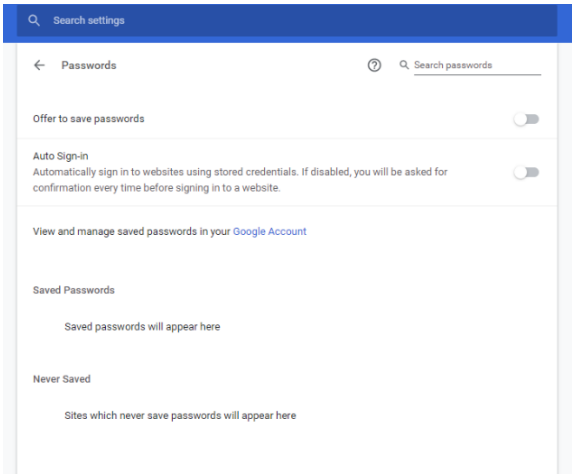
1Password Tutorial: https://www.youtube.com/watch?v=y6uPNnlwP1g
LastPass Tutorial: https://www.youtube.com/watch?v=SndS8zfXjSo

Chrome[1]: Click the three-dot menu in the top right of the browser and click **Settings,** then click **Passwords.**



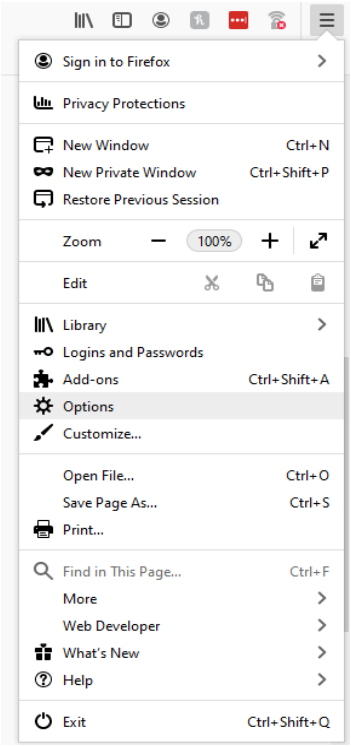


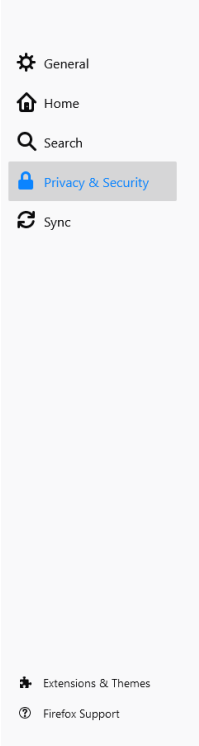
Make sure that *Offer to save passwords* and *Auto Sign-in* are unchecked and delete any saved logins.



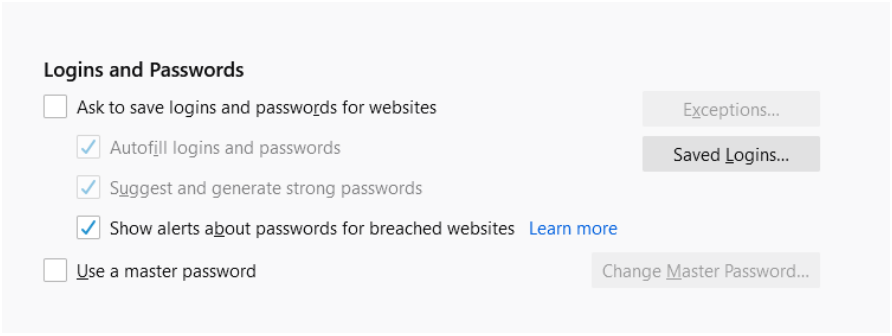
[1] The Apple Safari browser is a popular, reputable browser, but should similarly be secured by the end user. A good site for this is: https://www.imore.com/how-manage-privacy-and-security-settings-safari-mac

Firefox: Click the three-bar menu in the top right of the browser then click **Options** and go to **Privacy & Security**.

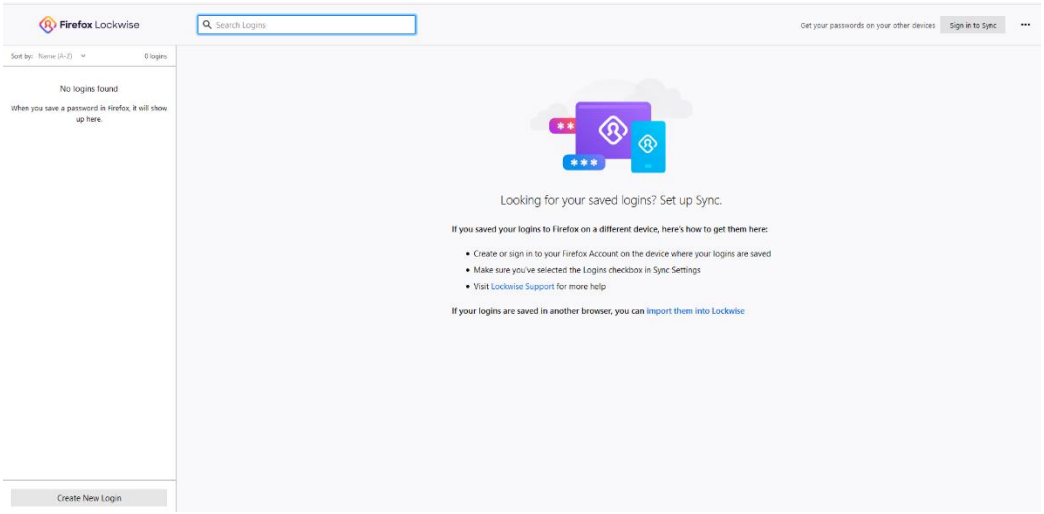




Go to **Logins and Passwords** and uncheck *Ask to save logins and passwords for websites,* then click **Saved Logins:**



Delete any saved logins within the browser:



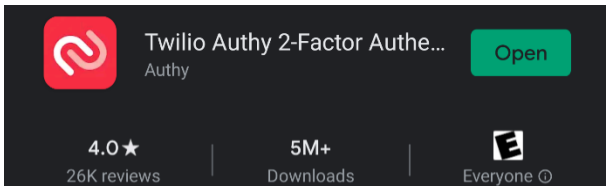
Multi-Factor Authentication

3. **(5 Points)** Use multi-factor authentication (MFA) and note ***this might be the most important step you take!*** It's now well known that usernames and passwords aren't enough to securely access online services. A recent study highlighted more than 80% of all hacking-related breaches happen due to compromised and weak credentials, with three billion username/password combinations stolen in 2016 alone[2]. As such, the implementation of MFA has become a necessity. Generally, MFA aims to provide an additional layer of security to the relatively vulnerable username/password system.

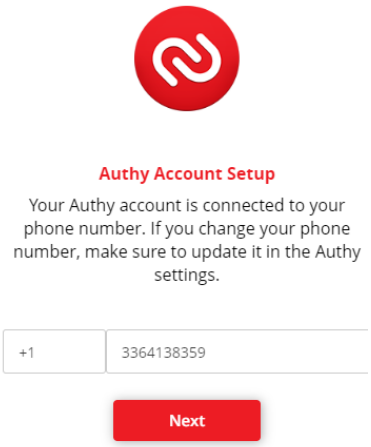
   Be careful not to fall prey to SIM swap scams! One of our colleagues uses an old phone that can only connect on WiFi (via VPN, below) and uses the Authenticator, Okta, or VIP access tools for MFA (e.g., MS Authenticator), which is far more secure than relying on SMS-based MFA (which can easily be defeated by a moderately capable hacker). If remote, this colleague can access the internet from his second device using his primary phone as a hot spot. So, the attacker would have to steal both devices, key credentials, and know how this set-up works. No fun carrying two phones, but it's secure and quick. Finally, make sure you turn on MFA for your password manager and EVERY site that supports MFA!

[2] https://thenextweb.com/news/hackers-cracking-two-factor-authentication-security-syndication

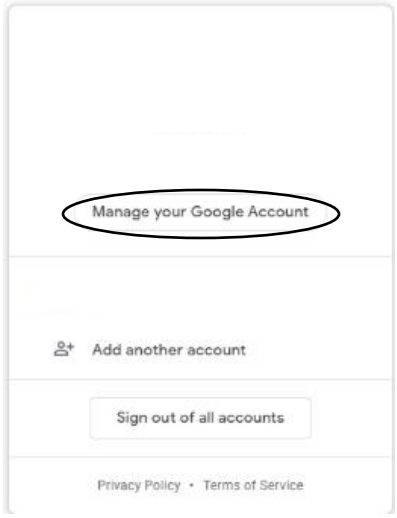
How to set up Authy (MFA application): Download Authy on either your Android or Apple device:

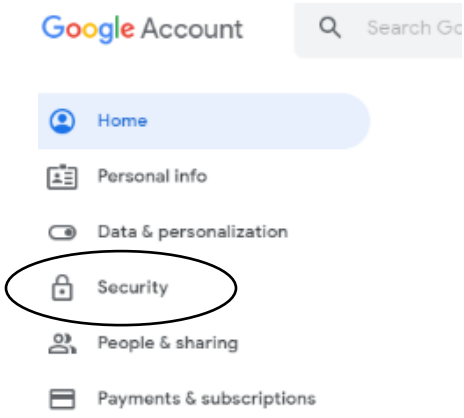


Set up an account with your phone number and email (at right):

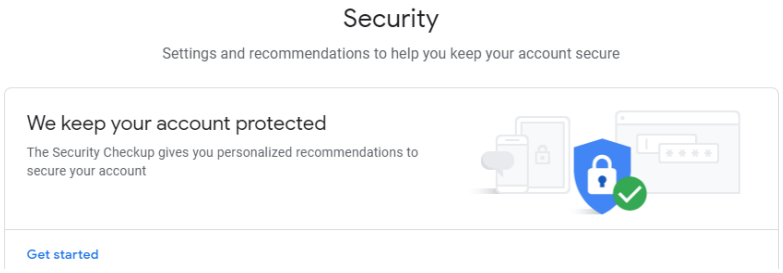


Now you can add MFA to accounts. Here is how to add MFA to Gmail: click on **Manage your Google Account,** then click **Security** on the left side.





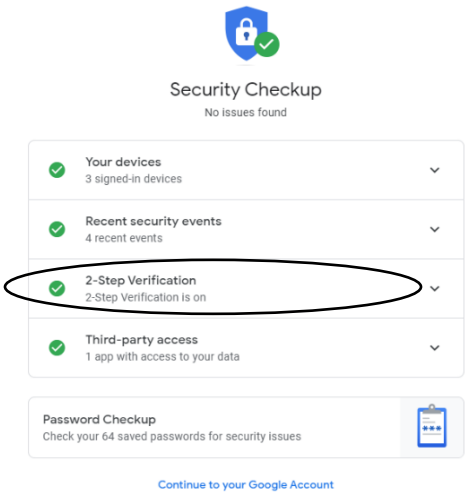
Click on **Keep your account protected** (above).

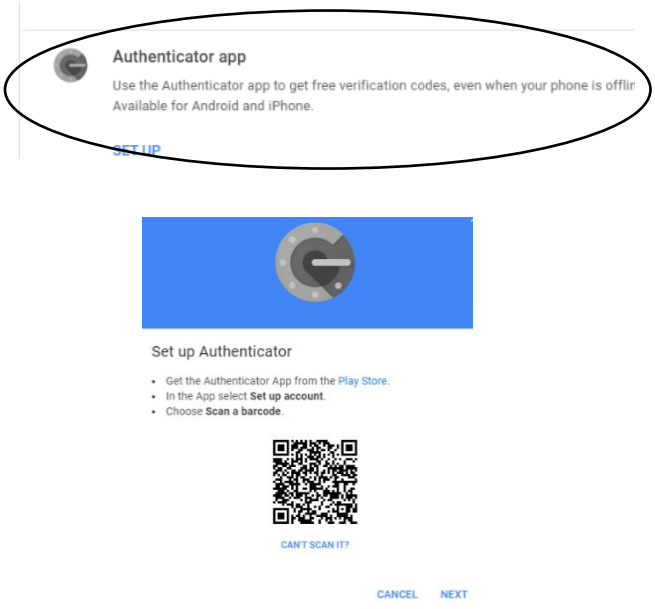


Click on **2-step Verification** then find *authenticator app* and click **SET UP.**

Select which kind of phone you have then the barcode should appear.

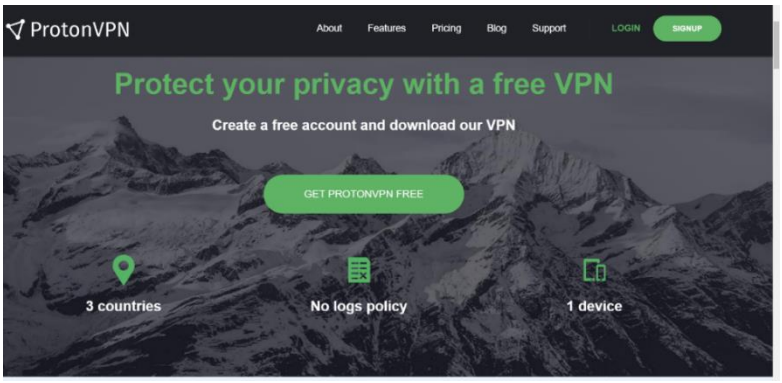
Now go to your Authy app in your phone and press **add account,** then **scan barcode.** Continue by setting up a backup password and save the account. Now when you log into your Gmail you will have to put in the code that loads in Authy in order to get into the Account. The steps are similar for most other accounts that have the possibility of MFA.



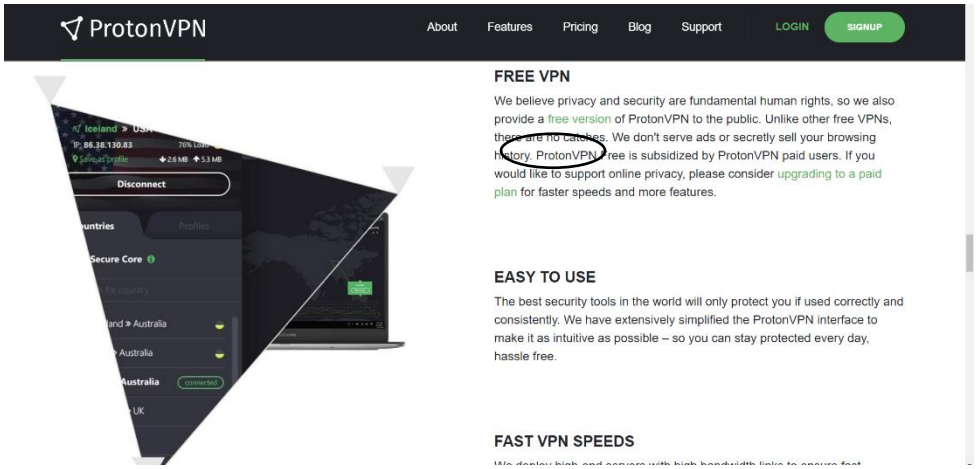


Virtual Private Network (VPN)

(2 Points) Always use a VPN (e.g., ProtonVPN) when in a public space – heck, we just set it up to automatically run all the time (starts up when your computer/phone do)! Set it up to automatically initiate a secure connection EVERY time you use your computer.

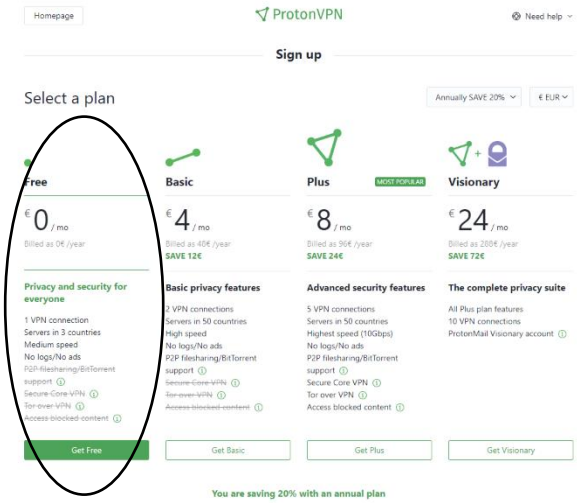


Example (but there are many free or low-cost services out there) for ProtonVPN: Go to the ProtonVPN website, scroll down and click on **Free Version (we always like free when it's a really good, secure service)**

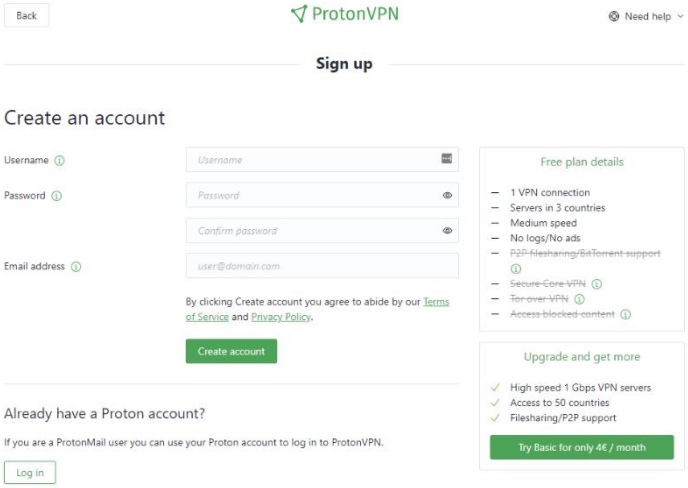


Click on **GET PROTONVPN FREE**

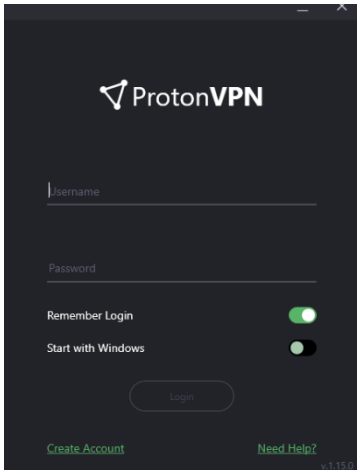
Click on **Get Free:**



Create an account
Download according to the operating system you are on (Windows or MacOS):



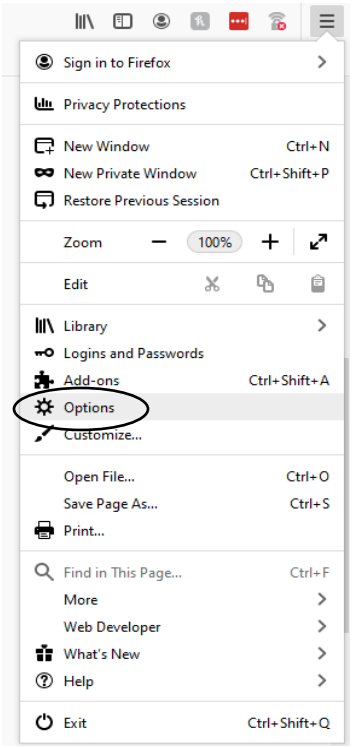
Login with the account you just made and connect to a server:

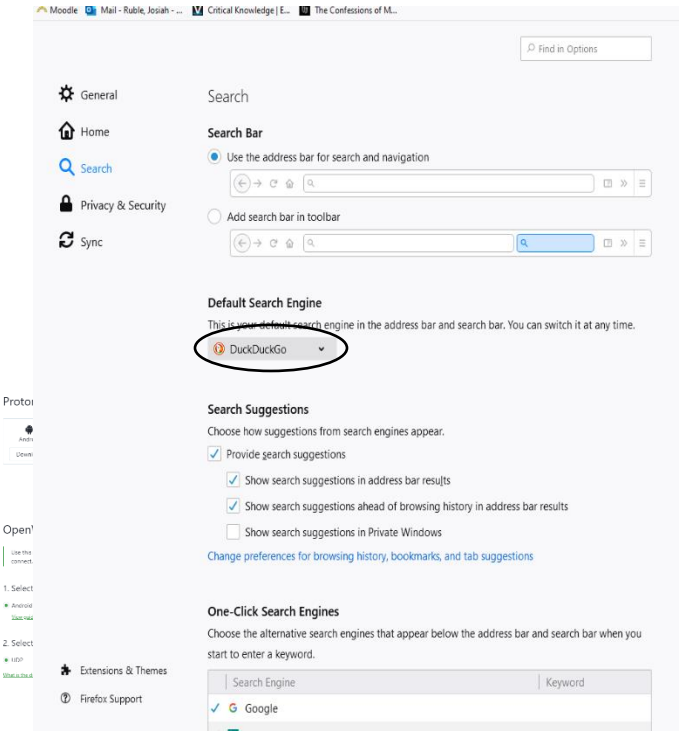


Secure Web Browsing

4. **(3 Points)** Use a secure browser such as Brave (not Edge, Chrome, Safari, etc.) and don't accept the ads and "digital currency" program. Also, use a secure search engine like DuckDuckGo or Searx.

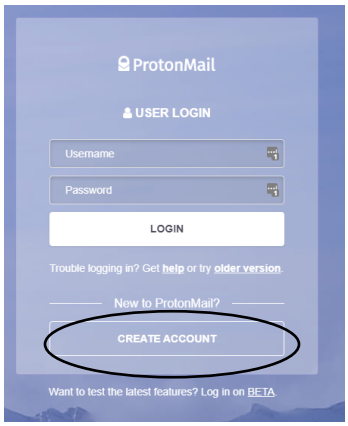
   Add DuckDuckGo by clicking on the three-barred menu in the top right of your browser. Click **Options,** then **Search,** and make the default search engine DuckDuckGo.



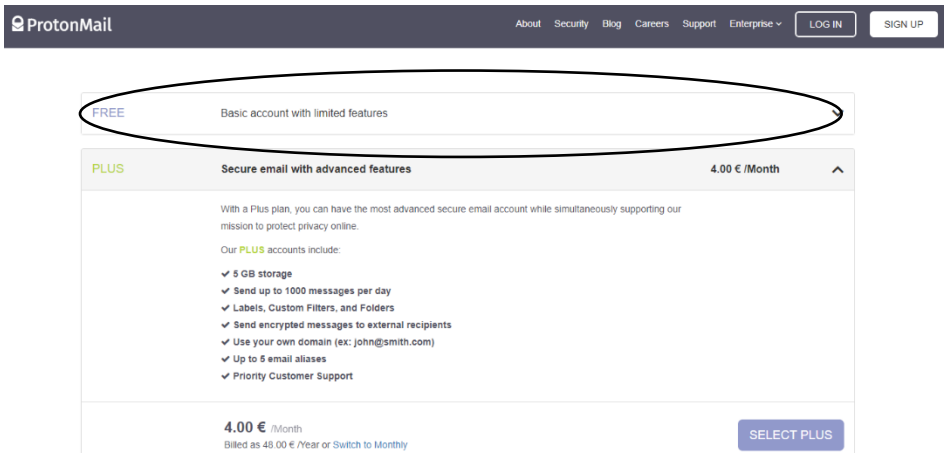


Secure Communications

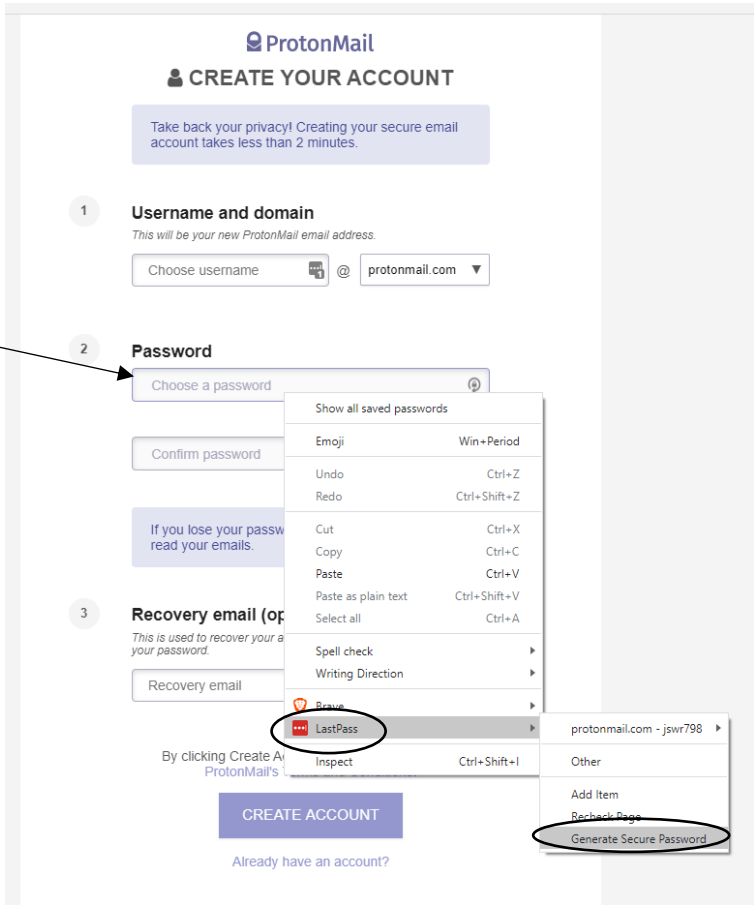
5. **(1 Point)** Use secure methods of messaging whenever possible (e.g., Signal, CellCrypt, or ProtonMail). For example, here are steps for our favorite: ProtonMail. First, user your private (remember step 5 above?) browser to search *ProtonMail.* Then, go to their home page and click **Create Account** (image at right)**:**



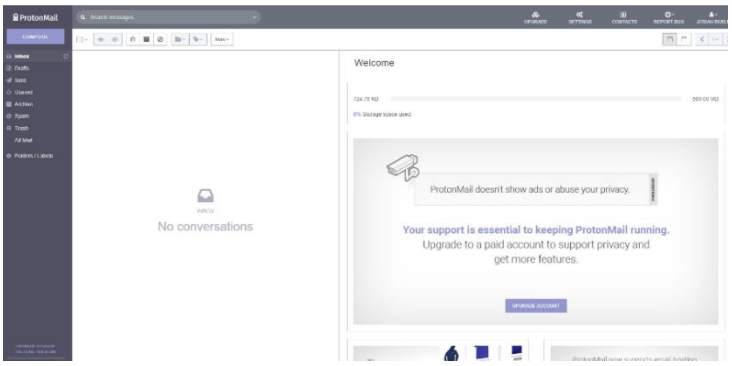
Click on the **Free** service:



Create an account with a strong password generated by LastPass and a recovery email:



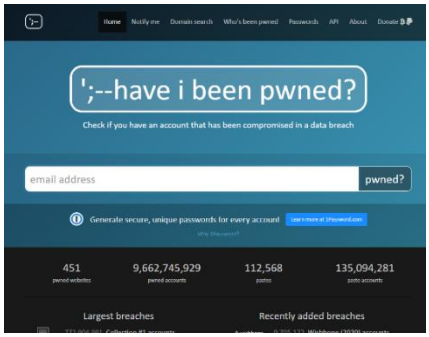
You now have a secure email address (inbox view at right). The free version is somewhat limited so use it for important company information or personal information.

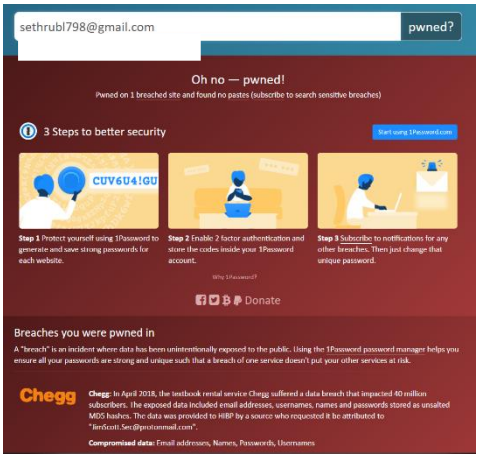


Securing Your Credit

6. **(1 Point)** Secure your credit (i.e., credit freeze through the three major agencies; https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs) and see if your information (e.g., email, credit cards, passwords) have been leaked/stolen (e.g., https://haveibeenpwned.com/).

   Have I Been Pwned? Click on the link above and search your email address (screen shot at right). If your accounts linked with that email have ***not*** been compromised the page will be green. If an account has been breached, the page will be red and show you what was breached.





Data Protection - Backup

7. **(2 Points)** Always have your core data automatically backed-up (e.g., to 2nd drive, Google Drive, OneDrive). Get extra credit if you back-up to two different places and one of those is "air-gapped", meaning once the backup is done, it cannot longer be accessed by another computer (e.g., via the internet) .

Total Score

Well, how did you do? Add up your scores from above and see how you rate with our table below.

Security Score	
0 2	No Security
3 5	Little to No Security
6 8	Little Security
9 11	Some Security
12 14	Secure
15 17	Highly Secure

Note that your personal cyber security is a never-ending journey. Please go back and review areas you can revisit to become more secure. Also, come back to our Carolina Cyber Center web site to look for updates (and send us suggestions)!