Cybersecurity 101: 5 places to start to be more safe online

Setting up your devices

- Password protect all of your accounts, especially the ones with superadmin privileges
- Encrypt all of your drives
- Turn on Firewall
- Turn on all location based tracking (Find My Device)
- Install virus protection software (even if you have a Mac)
- Scan your devices regularly
- If your computer is running slow, know who to ask to find out why.
- Avoid shared logins and reused passwords on your devices.

Recommended Software

- Avast
  - Free!
  - Easy to use
  - Doesn't slow down your computer
  - Autoscan

Passwords and Password Managers

- Passwords should be 15+ characters, should include uppercase, lowercase, numbers, and punctuation and can be either a series of multiple words or randomly generated characters.
- Password managers will help you keep track of these and make accessing them easy on all of your devices.
- Storing other sensitive information on a password manager, including credit cards, passports/IDs, and banking information, should be encouraged whenever possible.
- Password managers also make onboarding and offboarding staff much more seamless.

Strong Password Examples

- Pick 4-5 Letters (JABL) and then make a phrase using words that start with each of those letters. Add a number or punctuation if it makes sense.
  - Job$Apples4Ballet!League
  - !Jumping-Activists-546-Boron-Love
- Random characters
  - xAWcsM_nn7uMkvk-y
  - mhyVj98LNWR*CabZP

Recommended Password Managers

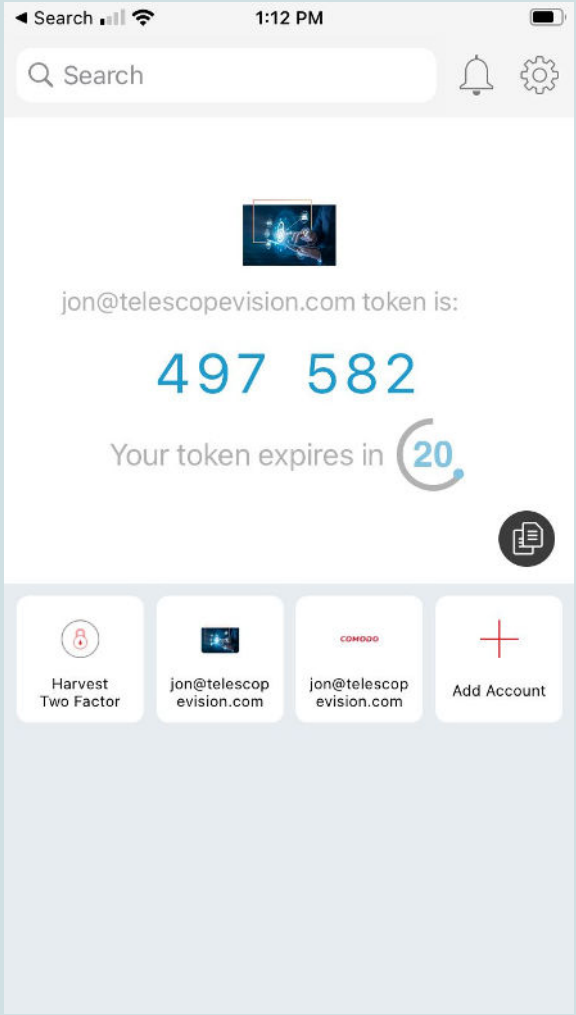
- 1Password
- LastPass
- Dashlane
- Remembear

Multi-factor Authentication

- **Multi-factor Authentication** (MFA) is a great second line of defense if one of your passwords is compromised.
- Most platforms offer a MFA option which can be turned on for all users of your accounts.
- At the bare minimum, email, financial and CRM platforms should have MFA turned on for all users.
- You can use an app like Authy to keep all your MFA codes in one place.

MFA Apps

- Authy is a great app to store all of your MFA codes in one place
- Instead of getting texts from random numbers, your codes will be available right away and reset every 30 seconds.
- And it's **free** and **encrypted**!

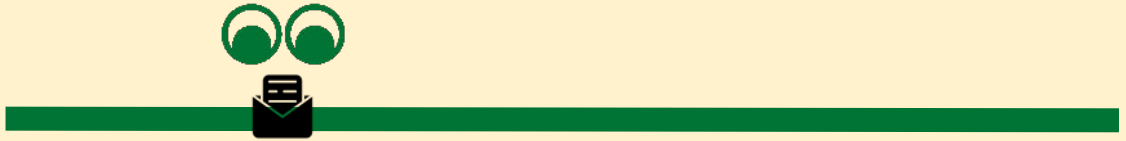


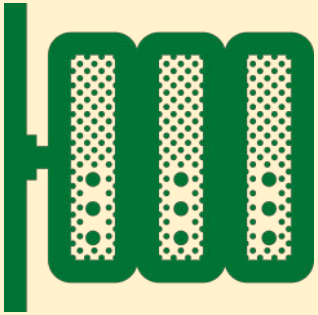
VPNs

The Internet :

Your Computer

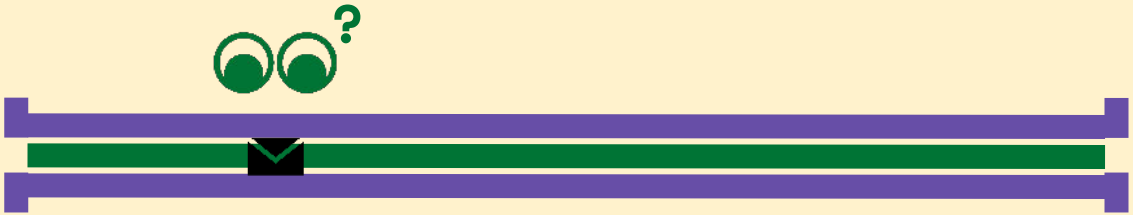
ISPs, trackers, hosting, etc.

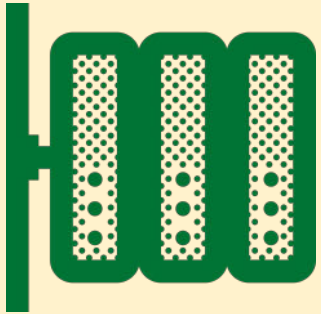




Servers where data is stored

Activity on the **Internet** is visible to internet service providers, advertising trackers, hosting services, and governments. A VPN hides the content of your message and shields you from third party spying.





Encryption via VPN

VPNs

There are many providers for VPNs and almost all of them work the same way. Here are a few recommendations to start your research.

- ➔ Tunnelbear
- ➔ Avast VPN
- ➔ ProtonVPN

Phishing and threat protection

Phishing [pronounced fishing] is a form of deception where a hacker attempts to impersonates a service or person in order to gain access to passwords, information, or data or to install malicious software.

Common phishing attempts may come as an email that is similar to a colleague, a link that looks like a service you use (Microsoft or GSuite are most common), or a login portal that mimics platforms you are familiar with. This is also known as **spoofing**.

What you can do to prepare for phishing

- ➔ Host a training with a certified cybersecurity professional. Encourage staff to share phishing threats with leadership and discuss during staff meetings.
- ➔ Practice makes perfect! Use a service like KnowBe4 that sends spoofed emails to test employee readiness.
- ➔ Check spam and email settings to weed out potential phishing threats.
- ➔ Never, ever, click links in emails if you don't know the sender.
- ➔ Double verify all requests for information on two platforms (email + phone, Teams/Slack, or an encrypted messaging app.

Executive Summary

1. **Setting up your devices** correctly secures your data in the event of a loss or theft.
2. Using **strong passwords** and an **encrypted password manager** ensures your logins are easy to access for those who need them and more difficult for a malicious actor to force into.
3. **Multi-factor Authentication** (MFA) is a good backup in the event of a phishing attack or password leak.
4. **VPNs** provide an added layer of privacy from other people on public or insecure networks.
5. **Phishing preparation, training, and monitoring** can help your organization know the common tricks hackers use to deceive you.

About and Contact

Telescope Vision is a nonprofit technology consultancy and IT services provider located in North End, Detroit, Michigan.

Our goal is to support nonprofit organizations to be more safe, efficient and agile as work and programming become hybrid in our sector. We do this by providing sector expertise and breadth and curating our services to your organizational needs. Everything we do is designed with each individual client in mind.

Contact:
Jonathan Riley
jon@telescopevision.com