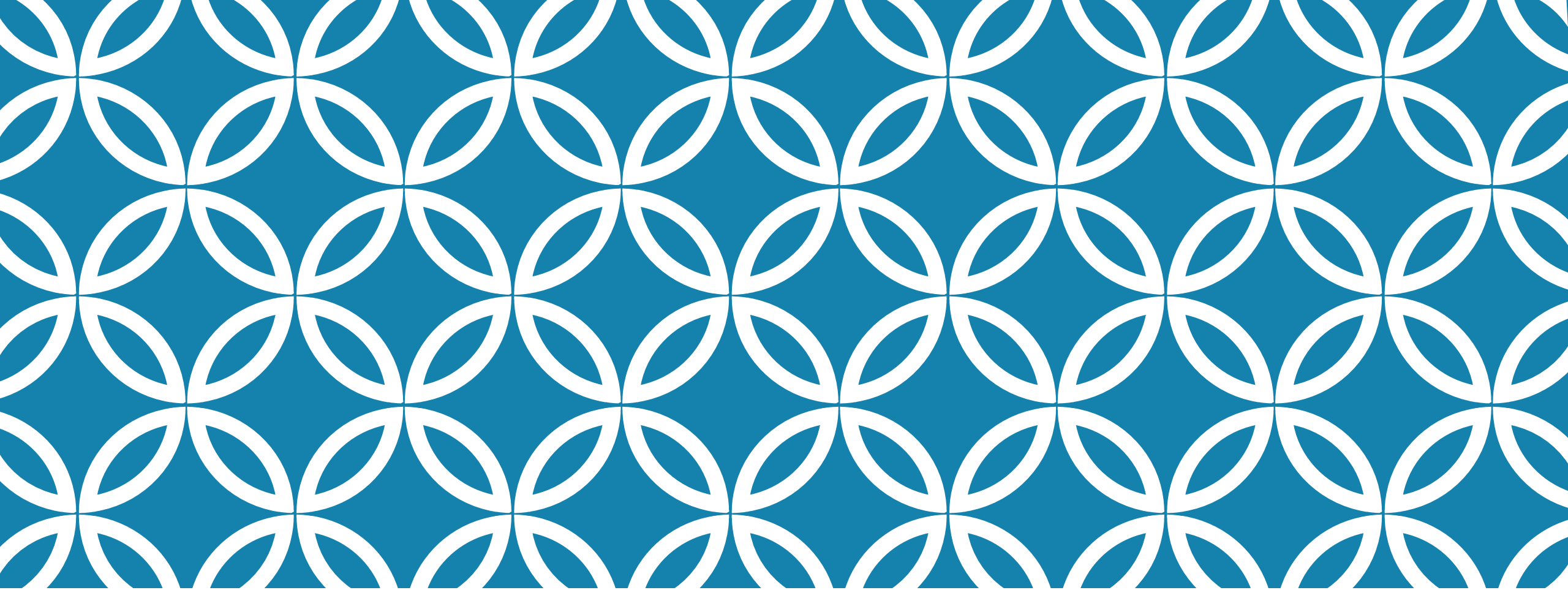


TIPS FOR PROTECTING YOUR TECH

Paul Stoddard

June 7, 2021

THE MAIN POINTS

1. Passwords – protect them
2. Phishing – watch out of suspicious emails (and phone calls)
3. Back up your data
4. Software – keep it up to date
5. Anti-virus software
6. Ransomware
7. Identity Theft
8. Protect your mind - watch out for false news and information

PASSWORDS

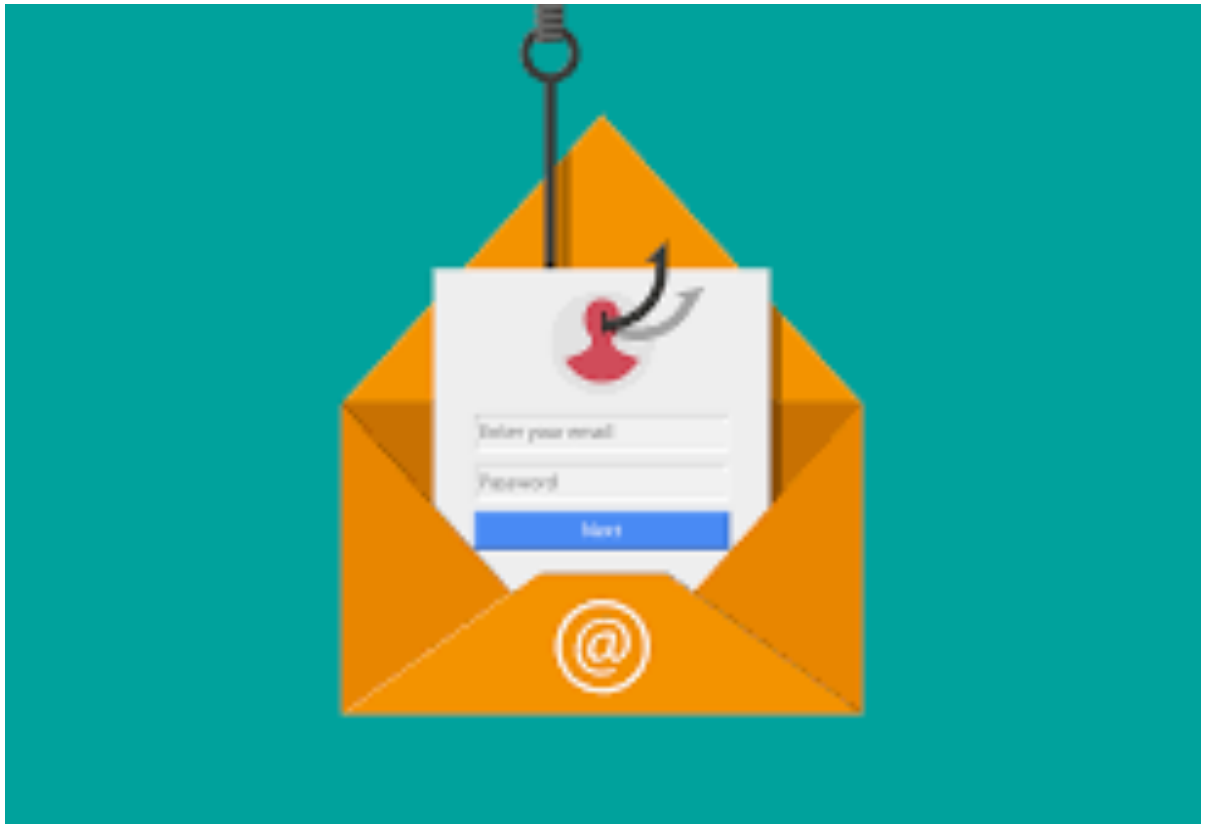
Use different passwords for different sites.

Make them hard to guess:
(UPPER & lower case letters + numbers + special characters),
or a short sentence.

2 factor authentication (most financial websites use this). This is usually a text to your cell phone with an extra code.

Because they're hard to remember, use a password manager:

- A spreadsheet that is locked by a password that is hard to guess
- Keychain on iMacs
- Or buy one (https://www.pcmag.com/picks/the-best-password-managers)



PHISHING

Hackers focus mainly on large organizations. For small fries, they use phishing.

Phishing is someone trying to trick you into giving up your personal information.

It comes mainly through emails or phone calls. Watch out for scams.
Never give your personal information (SSN, birth date, bank accounts, passwords, etc).
When you get unexpected emails, don't open attachments or click on links.

Use email features for handling junk mail.

BACK UP YOUR DATA

Backups give you protection in case your hard drive breaks. A backup can also save you if you get ransomware.

- Cloud backups (such as iCloud)
- External hard drive
- Some operating systems come with software to manage backups (Time Machine on iMacs)

KEEP SOFTWARE UP TO DATE

The main types of software are:

- Operating systems such as Windows, MacOS, iOS, Android
- Apps like Word, Zoom, games
- Cloud software like Google docs, Dropbox, etc. (you don't need to update cloud software)

Microsoft, Apple and other software companies are constantly updating their software to add new features and protect from malware. They usually prompt you to install updates. (But watch out for fake emails claiming to have an update.)

Sometimes you must pay to get the latest version. Eventually, the company that makes the software will stop supporting old versions and you really should upgrade when that happens.

ANTI-VIRUS SOFTWARE

- Examples: Norton, McAfee, Malwarebytes, etc.
- Many have a free version. These are available to convince you to get the paid version. The paid versions are are always up to date. They run on your computer in the background and catch bad things (like emails) before they can mess up your machine.
- There is less malware out there for Apple products, but there is some.
- https://www.pcmag.com/picks/the-best-android-antivirus-apps
- https://www.pcmag.com/picks/the-best-antivirus-protection
- https://www.pcmag.com/picks/the-best-mac-antivirus-protection

RANSOMWARE

- What is it? A type of malicious program (malware) that encrypts your files so you can't use them. You must pay the bad guys to get the key that will unencrypt your data.
- How do you pay? Bitcoin or other crypto-currency. (Bad guys like them because they can't be traced.)
- How do you protect yourself? The same way as you do against other malware – be careful, backup your computer, use good passwords, use anti-virus software.
- Wired article on how to protect yourself.
- US Cybersecurity & Infrastructure Security Agency ransomware guidance.

IDENTITY THEFT

- When someone steals your identifying info (such as Social Security Number), they may try to open new loans or credit cards in your name. You end up with the bills.
- Check your credit card statements carefully and call the credit card company immediately if you see suspicious charges. You shouldn't have to pay if you call them right away.
- You can pay for identity theft protection (for example, "Lifelock"), but Consumer Reports says it's not worth it.
- US government advice on identity theft
- You can lock your credit to prevent thieves from using your personal information. There are 3 major credit agencies - you have to request locks on each one separately. You can unlock it yourself when you need to get a loan.
    1. Equifax
    2. Experian
    3. TransUnion

PROTECT YOUR MIND: NEWS SOURCES

- Never trust news found on Facebook, Twitter or other social media!
- Watch out for "free" news. Be willing to pay for a few good sources. Our country needs good journalists!
- The diagram on the right shows the quality and bias of various news sources. (There are many versions of this.)
- MediaSmarts has this tip sheet on how to recognize false content.