STACIE FARMER - OPENWEST 2019

CYBERSECURITY BASICS EVERYONE NEEDS TO KNOW

WHO AM I?

- Stacie Farmer
- Owner of Mayet Security
  - Helping everyday people learn cybersecurity fundamentals
- Programmer, former community leader, endless learner

3 RULES TO REMEMBER

- Life is risk
- You will be attacked (at some point)
- Nothing can be 100% secure

I got into this field so I could feel safer using technology

- Was tired of feeling scared but not knowing what I should be scared of
- Part of why I created this talk
- Research uncovered these 3 rules
- Being alive means dealing with risk
- You will be attacked, or more likely already have been
- Because nothing can ever be 100% secure
- Burden off your shoulders. Don’t have to be perfect at cybersecurity.
- Learn a little, try some things. Learn some more and try some more. You just have to take it a few steps at a time.
- This talk will be a little like drinking from a firehose. Take what you can and try to implement at least a few things.

WHY? WE'RE ALL CONNECTED

- System was built with presumption of trust
- Everything's vulnerable
- Attacks are happening all the time

Why do you need these cybersecurity basics?

- Because our systems suck at security. Built with trust - small office with trusted people/devices
- The foundation of the internet implied trust, which now seems like a terrible idea
- So everything is vulnerable because it's so trusting
- We're connected globally so attacks happen all the time
- Everyone is affected by cybersecurity on a level like never before. It should be a requirement that we have a basic foundation of cybersecurity basics so we can use technology without fearing attacks.

WHAT DO THEY WANT?

- Assets (routers, servers, devices)
- Information (identity theft, social engineering/phishing)
- Assets + Information = **Money**

- *Others*:
- Revenge
- Political Motives
- Lulz

Why are malicious attackers doing this?

- They want our devices - assets - to make them lots of money.
- Routers to distribute malware. Smart TVs for pay-for-hire DDOS company. Mail server to send spam.
- And they want information to make them lots of money
- Database to steal customer info. Malware on device to gather TONS of personal info.
- Billion dollar businesses are built on gathering your info, curating it, and selling it to other companies.
- Or used in social engineering, great for individual attacks and cyberwarfare {Example of Ukraine social engineering Russian military to get military secrets. Equifax data not being sold on black market. Office of Personnel Management data being stolen}
- Attacks also happen for revenge, to make political statements, or just cuz they can
- Sometimes, it just happens and you never really know why.

WHAT DO THEY WANT?

“Every VM [virtual machine] is lost. Every file server is lost, every backup server is lost. Strangely, not all VMs shared the same authentication, but all were destroyed. This was more than a multi-password via ssh exploit, and there was no ransom. Just attack and destroy.”

https://krebsonsecurity.com/2019/02/email-provider-vfemail-suffers-catastrophic-hack/

In February this year, VFEmail had all their primary and backup data in the US completely wiped out. 18 years worth of customer’s email, gone. No reason why, that they could see. Just all the data in the US, gone.

Most of the time, malicious hackers want money. But every situation is unique.

PREVENT ATTACKS – MULTI FACTOR AUTHENTICATION

- Enable MFA ***anywhere*** and ***everywhere*** you can

WHAT IS MULTI FACTOR AUTHENTICATION?

- What you know *(username, password, pin)*
- Who you are *(fingerprint, facial scan, iris scan)*
- What you have *(physical token/key)*

So what's the most valuable thing you can do right now?

- Enable multi-factor authentication, also called 2FA, on any account you can
- 3 things can be used to prove you are who you say you are
- At least 2 must be used to prove you are who you are (2FA). More is better.
- It's too easy to get one of the factors. Data breaches are happening constantly. GDPR means we hear about them now.
- 2FA makes it harder for someone to illegally access your account. They can still do it, but it's just a little bit harder.

PREVENT ATTACKS – MULTI FACTOR AUTHENTICATION

- **Best MFA: Physical key**
  - Prevents against:
    - *compromised credentials, SIM swaps, phishing sites*
  - Doesn't prevent against:
    - *theft of the key*

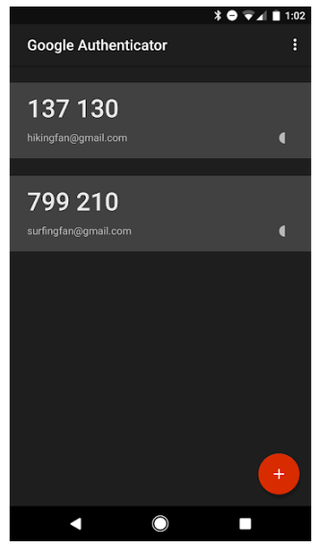
https://en.wikipedia.org/wiki/YubiKey

Let's talk about the 3 forms currently available

- Best form, currently, is a physical token or key
- Example here is YubiKey - USB slot and has bluetooth capabilities
- Protects against…
- Doesn't prevent against…
- Best option if you have it
- Don't have it or don't want to spend $50 on it…

PREVENT ATTACKS – MULTI FACTOR AUTHENTICATION

- **Pretty Good MFA: Authentication app**
  - Prevents against:
    - *compromised credentials & SIM swaps*
  - Doesn't prevent against:
    - *phishing sites*



https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

Next best option is using an authentication app on your smartphone

- Just needs a QR code from the website to set it up
- Shows you a code for each website that resets after a minute or so
- Prevents against…
- Doesn't prevent against phishing sites - explain…
- Protects you from a lot of things, but what if you don't even have that option…

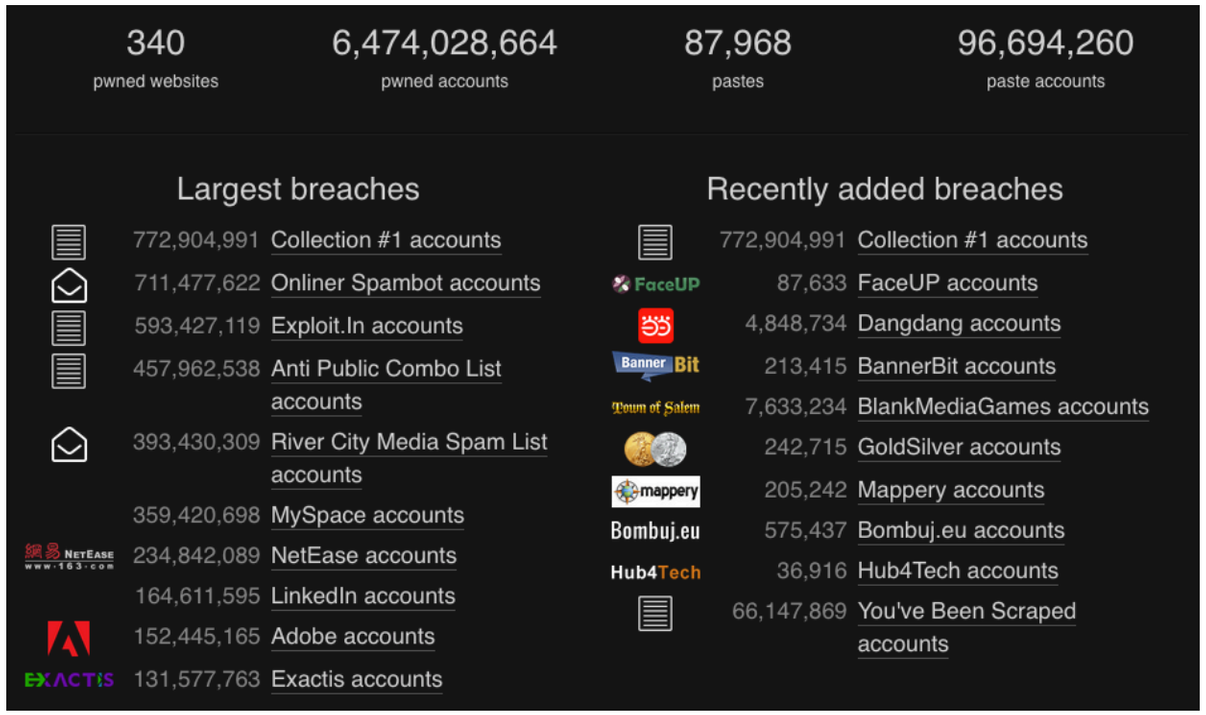
PREVENT ATTACKS – MULTI FACTOR AUTHENTICATION

- **Good Enough MFA: SMS Messaging**
  - Prevents against:
    - *compromised credentials*
  - Doesn't prevent against:
    - *SIM swaps, phishing sites*

We use the good enough option - SMS/Text Messaging

- If it's your only option, it's your best option
- Protects against…
- Doesn't protect against…phishing sites; SIM swaps (explain)
- January - Michael Terpin, 3 million cryptocurrency tokens (about $24 million at the time) stolen. Rogue AT&T employee swapped SIM card with international crime gang. {reference: https://threatpost.com/att-faces-224m-legal-challenge-over-sim-jacking-rings/136645/}
- Use VOIP number, but protect that account with stronger forms of 2FA
- Still better than nothing. Will stop compromised credentials {switch to next slide}
- Set it up wherever you can

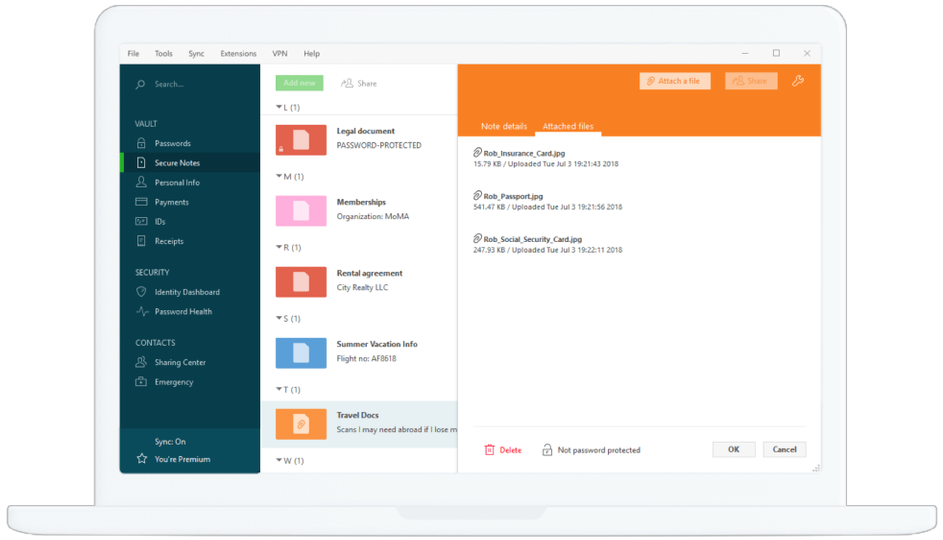
HAVE I BEEN PWNED [DOT] COM – ANSWER, YES YOU HAVE



This is from haveibeenpwned[dot]com. As of January 24th, there were almost 6.5 billion pwned accounts. Those are just the ones Troy Hunt is aware of. There are plenty more out there and more to come.

{switch back}

PREVENT ATTACKS – PASSWORD MANAGER



AccompanyCapsuleLaxativeObtrusiveFiltrateRockband

EFF Dice Passphrase - https://www.eff.org/dice

You're going to use 2FA, especially on sensitive accounts

- But where do you store those hundreds of accounts? In a password manager
- Create one account that has a strong password. Use passphrase (link above and example - explain)
- Enable 2FA on this account - using a strong factor - and store all your other logins
- You can store notes (like security question answers), backup codes, and files
- Have strong password generators
- Cloud based to be accessed anywhere; have browser extensions to autofill login info
- Still a security risk so do your research first

PREVENT ATTACKS – PASSWORD MANAGER

- **Use a password manager**
  - Stores all your unique & strong credentials
  - *Prevents against:*
    - Brute force attacks & credential stuffing
  - *Doesn't prevent against:*
    - Phishing attacks, data breaches, lost master password, spyware

Once you've stored all your websites, you will only use unique, random, strong passwords for every site

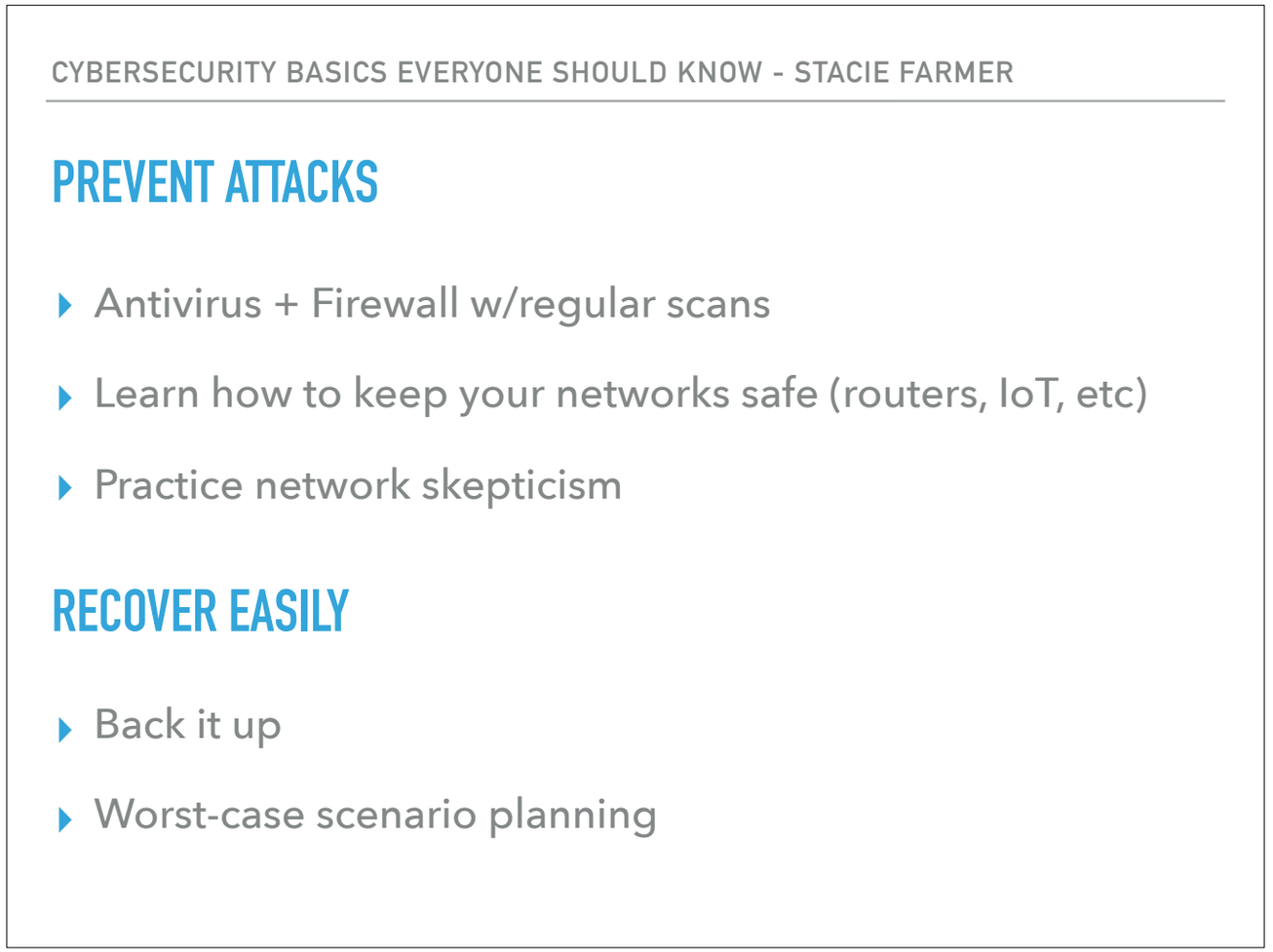
- Attackers are using credential stuffing to take compromised credentials from one site and try them on another
- Hulu account was attacked this way
- So unique passwords on every site with 2FA enabled where you can
- Also prevents brute force attacks where they try a list of passwords to get in
- Can't prevent phishing attacks, but browser extensions can help - watch out for attack using Google translate
- Can't prevent data breaches - even they've been breached but nothing sensitive has been leaked…yet
- Can use a password manager just on your device. Still definitely better to use it than not.
- Can't protect you if you share or lose your master password. Can give you an emergency contact if there's someone you trust to have access if you lose it or pass away. Don't change your master password more than once a year. If you don't suspect a breach and you have 2FA, you're more likely to forget the password.
- Can't protect you from malware. Always use a clean computer

PREVENT ATTACKS – PII

- **Personally Identifiable Information**
  - Share as little as you can
  - Create disinformation (where legal)
  - Freeze your credit
    - https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
  - Monitor accounts (including annual credit reports)
- Know who to notify
  - https://www.identitytheft.gov/

What can we do to protect our information?

- PII is Personally identifiable information - which nowadays is basically anything about us
- Share as little as you can. Most businesses ask for it but don't need it. Don't share it.
- Or share false information - disinformation - where it's legal. Must provide accurate information to government, legal and police, and for obtaining financial credit. Many companies require it for their terms of service. But if they don't need it, don't give it to them.
- Use false information, not someone else's information. That's identity theft and is a crime.
- Great for "security questions". Anyone can find HS - put something random instead and save in password manager.
- Freeze your credit. Free and relatively easy - about 30 minutes. No one can pull a credit report for you where it's frozen so much less likely to open a new account in your name.
- Link gives you instructions. Store information in password manager so you can unfreeze it later.
- Freeze kids' accounts too. Theirs is more valuable - longer history with nobody watching.
- Monitor accounts - financials and report right away. Annual credit reports - still free if credit is frozen though you may have to mail info.
- Pull all 3 at once, if haven't in a while. Report any problems. If clean, a year from now pull one - Equifax. Wait 4 months then pull another - TransUnion. Wait 4 months then pull another - Experian.
- If you're a victim of identity theft - check out this website to help you get back on track. Great resources from FTC.



Oldie, but still good advice

- Have an antivirus, everyone, and run regular scans. Enable your firewall
- Everyone has a home network now. Learn how to set it up and secure it
- Buy a decent router. Cheaper usually means less secure. Change password immediately and update firmware regularly. Disable UPNP if you don’t need it. Find out if you have any ports open on your WAN and why. Learn how to configure your router properly.
- Know every device that should be on your network. Kick off anyone else. Create a guest network - for guests but maybe also for IOT devices
- Research IOT devices before bringing them into your network. Make sure they can be secured. Many products have hard-coded passwords. Once online, it can take minutes for your device to be pwned.
- Once an attacker is in, hard to spot and do a lot of damage
- Practice general network skepticism. Public networks - Keep your firewall on, folder sharing off, have an updated antivirus, and just use a VPN. Or don’t use them if you don’t have to.
- If you love it and/or need it, back it up regularly. Think of VFEmail - what’s the worst-case scenario for you? What can you do to avoid it?

PREVENT ATTACKS

KREBS'S 3 BASIC RULES

- If you didn't go looking for it, don't install it!
- If you installed it, update it.
- If you no longer need it, remove it.

https://krebsonsecurity.com/2011/05/krebss-3-basic-rules-for-online-safety/

Basic guidelines that are very valuable from Brian Krebs

- If you didn't look for it, don't install it. Includes software, updates, email attachments, and clicking on links
- All used to install malware (updates for MITM attack, links - or social media messaging for phishing sites)
- If you didn't go looking for it, don't install it
- If you installed something, keep it up to date! Very important. Back it up first, then update it within a week. If not, it will likely be used to attack you.
- If you don't need it, get rid of it. Old software, but also old libraries or WordPress plugins. Reduce the possible places you could be attacked.

CYBERSECURITY BASICS EVERYONE SHOULD KNOW - STACIE FARMER

ABSOLUTE BASIC CYBERSECURITY HABITS

- Enable MFA/2FA
- Use a password manager
- Have strong, unique, random passwords for each site
- Share very little info or disinformation where you can
- Freeze your credit & monitor accounts
- Antivirus + Firewall with regular malware scans
- Be skeptical of networks. Keep yours secure & safe.
- Back it up & Worst-case scenario planning

To prevent attacks, you will:

- enable 2nd factor authentication
- Use a password manager
- Set strong, unique, random passwords on each site
- Share little to no information about yourself or use disinformation strategically
- Freeze your credit & monitor your accounts (including getting your annual credit reports)
- Install and run your antivirus with regular scans. Set up firewalls on devices that have them.
- Stay skeptical of networks. Keep yours secure and safe and practice safe techniques like VPNs when you have to use a public network.
- If you love it, back it up and take some time to think of what a worst-case scenario looks like for your situation

3 RULES TO REMEMBER

- Life is risk
- You will be attacked (at some point)
- Nothing can be 100% secure

Remember our 3 rules: Life is risk, You will be hacked, and nothing is 100% secure. Whatever happens, it will be painful, but you will recover.

That’s all I have time for today. There’s much more, but we’ve covered at least the absolute basics you should be doing. What else can you do?

WHAT ELSE CAN I DO?

- Keep learning!
- **Blogs:**
  - Krebs on Security
  - Threat Post
- **Podcasts:**
  - Cyberwire
  - Security Now

Can keep learning! Always lots of interesting stuff to learn

- Krebs on Security great blog with interesting news stories
- ThreatPost has lots of up-to-date events
- Love me some podcasts
- Cyberwire is like ThreatPost with up-to-date events. About 20mins long & released every weekday
- Security Now is 2hrs long, released every Tuesday, but goes way more in-depth on things. Great for learning
- Wherever you're at is the perfect place to start. Pick one or two things and try them out. Keep doing that and you'll become more secure over time.