

# Cybersecurity for the Individual

Jack Parks, KQ4JP

Fayette County Amateur Radio Club

Fayette County ARES

# What do threat actors want from you?

- Your Identity (leverage your reputation)
- Your Bank Accounts (show me the money)
- Your Access to Things (keys to the kingdom)
  
- In the end, it is about **MONEY**

# Cybercrime and Money

- Cybercrime To Cost The World \$10.5 Trillion Annually By 2025
- 90% of security breaches in companies are a result of phishing attacks
- **Cybercriminals Stole \$1.8 Billion from Unsuspecting Older (50+) Americans in 2020**
  - More than doubled from 2016
- **Fraud & Extortion:**
  - provide personal and financial information;
  - give money or buy expensive gifts; or
  - launder money unknowingly.

# A tale or two....

- In 2013 Target lost almost \$200M (not including reputation)
  - Cybercriminals were able to steal 40 million credit and debit numbers and 70 million customer records.
  - It all started with a secretary at an HVAC company.
- In 2023, several Casinos in Las Vegas hit with Ransomware
- RiteAid - Jul, 7 2024 – 2.2 million customer records in 12 hours
- I received a phone call last month from “USAA Fraud Prevention”
  - Highly convincing – they had the script.
  - I was distracted....
  - They almost got me.

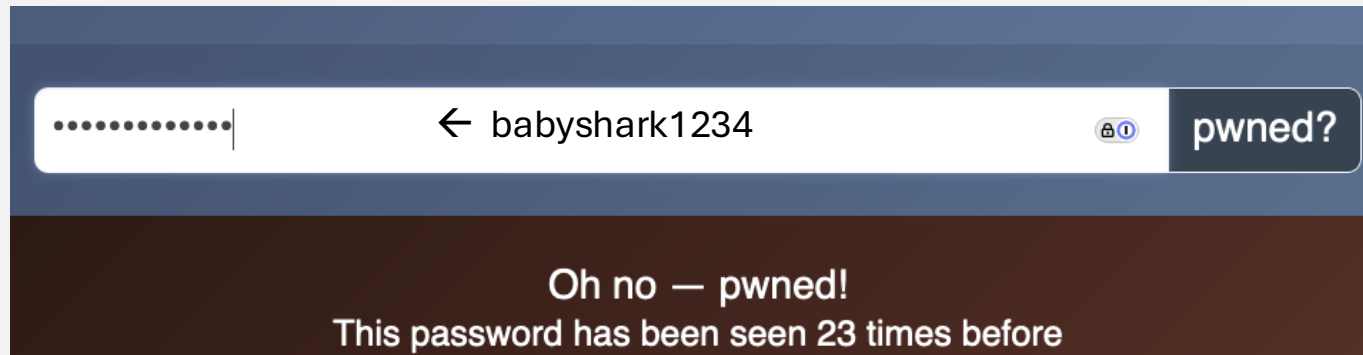
# Slow your roll

## **Urgency is what will get you....**

- Threat of collections against you
- Somebody needs financial help NOW!
- You forgot to pay that bill
- Your bank is closing your account today,
  - if you don't fill out this for, or
  - Sign in and verify immediately or
  - Your account was compromised and they are stealing all your money.
- This “opportunity” won't last forever

# You're compromised and don't even know it

- ❖ Most of your PII (Personally Identifiable Information) is on the dark web.
- ❖ Your email address is well-known
- ❖ Your “short” password has been compromised
- ❖ See for yourself - <https://haveibeenpwned.com/>



# Rainbow Tables

A rainbow table attack uses a pre-generated file containing hashes and their plain text equivalents to crack passwords stored in a database. If there is a match between a hash in the database and one in the rainbow table, the authentication is now possible, the password has been cracked.



.....| ← babys shark1234

Unlock 1Password

It would take a computer about

## 1 hundred years

to crack your password

## TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

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	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

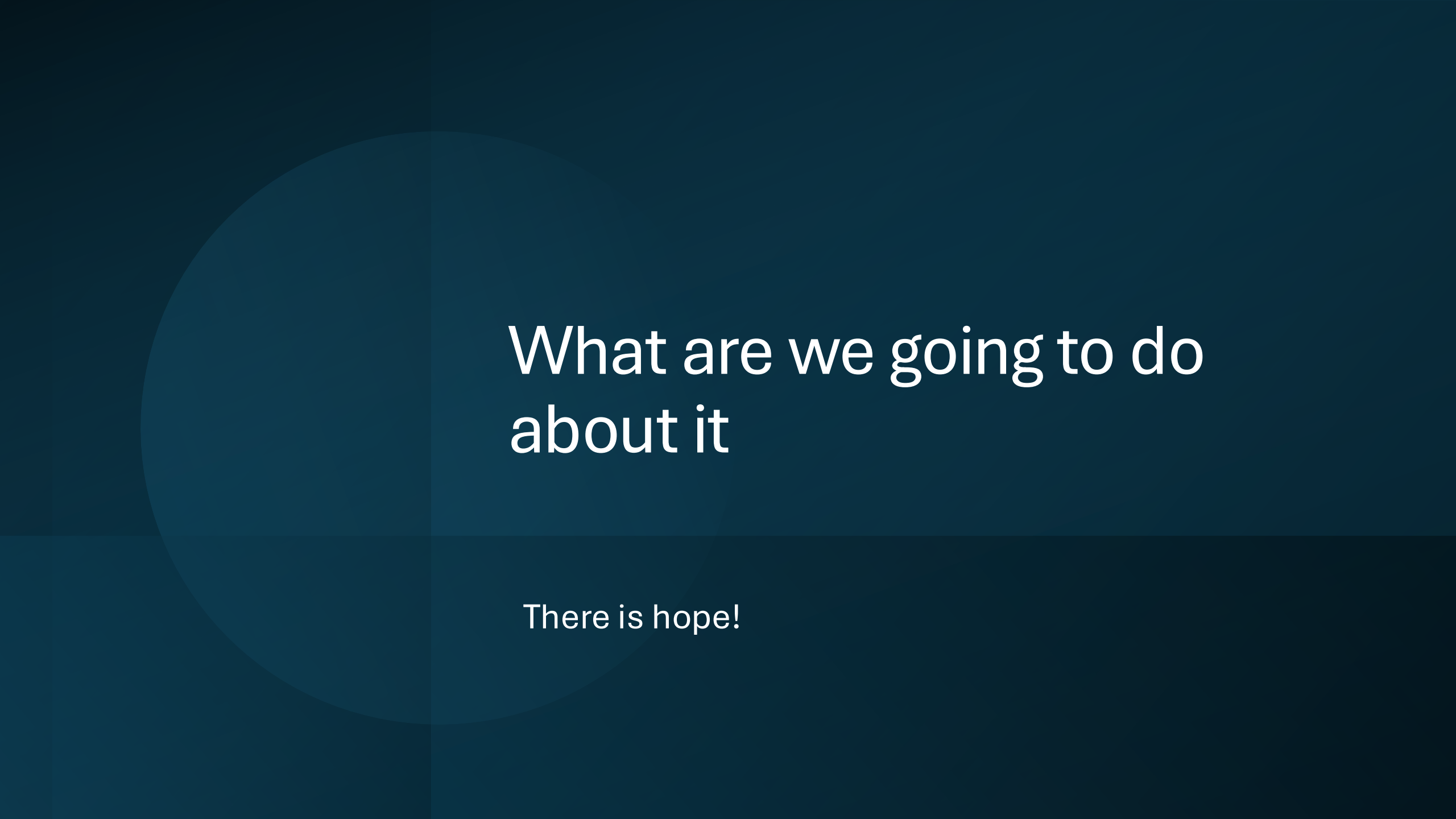


-Data sourced from [HowSecureIsMyPassword.net](https://www.howsecureismypassword.net)

# Other Things to Think About

- MFA bombing (also known as “push bombing” or “MFA fatigue”) is a brute force attack on your patience.
- SMS for two-factor authentication [2FA] is broken
  - People can clone your phone
  - SMS was never meant to be secure communication
- **Social Engineering:**
  - Is a tactic used by attackers to trick individuals into divulging confidential information. In the case of SMS-based MFA, attackers can contact the victim’s mobile service provider and impersonate the victim to get the SIM card associated with the victim’s phone number. With the SIM card, the attacker can receive SMS messages intended for the victim, bypassing the MFA process and gaining access to the targeted account.





What are we going to do  
about it

There is hope!

# A Thought on Email Addresses

- Have a **restricted** email address:
  - Financials
  - Family & Friends
  - Limited Use
- Have a **broad-use** email address:
  - Newsletters
  - Stores/Clubs/Affiliations
  - Subscriptions
- BONUS:
  - Separate email for Social Media

# Have a Good Password



## Long passwords are a necessity

Chicken-run.tuna-f1sh (21)  
Rebel.base2Death.star (21)  
1Happy2Dance3Penguin! (21)  
tzg4nvg1ycm4prv@AKZ (19)






## Never reuse a password

It doesn't matter how good it is

# Multifactor Authentication (MFA)

!!!USE IT!!!

- Physical – i.e. Yubikey
- Passkeys (Passwordless Sign in)
- Rotating single-use token
- SMS

username	pa[REDACTED].com
passkey	created May [REDACTED] 
password	..... Fantastic 
One-Time Password	974 • 539  12

Not endorsing!

How do I  
manage all of  
this?

## Password Managers

- 1Password
- Bitwarden
- <https://www.wired.com/story/best-password-managers/>

## Malware and Phishing Protection

- Malwarebytes
- Anti-virus programs don't work

## Browser Protection

# Make it Hard(er)

- Call people/companies back
- Kill the urgency
- (semi)Randomize username
- Use a username over an email address
- Variance (entropy) to remove predictability
- Long passphrases
- Use whatever MFA they offer

# A Word About VPNs



Highly recommended for public WiFi networks.




They secure the last mile and provide obfuscation.

Sites you log into will still know where you are, and social media cookies, trackers, and ads can build up an invasive profile of your browsing habits



If it's free - you are the product.



How does this apply to  
Ham Radio?



# Criminal Gain

- Identity
- Fraud
- Extortion
  
- ***Your callsign is a well-known entity***
- ***Public information is available in the FCC website (and others)***
- ***Hobbyist are "older" with "wealth"***
  
- Keep tabs using Google Alerts  
[www.google.com/alerts](http://www.google.com/alerts)

The screenshot shows the Google Alerts interface. At the top, the word "Alerts" is displayed in a purple header, with the subtitle "Monitor the web for interesting new content". Below this is a search bar containing the text "KO4WBM". A confirmation message states: "This will create an email alert for parks.jack.w@gmail.com." Below the message are two buttons: "Create Alert" and "Show options".

The "Alert preview" section contains the following text: "There are no recent results for your search query. Below are existing results that match your search query." Below this, there are two categories of results:

- NEWS**  
If the grid goes down, amateur (ham) radio works when all else fails - The Citizen  
The Citizen  
Remembering what I knew about the usefulness of ham radio, I decided to get my license the following year. Jack Parks (**KO4WBM**) and Bryan Macera (K7CPT) ...
- WEB**  
**REF030**  
dstargateway.org  
**KO4WBM**, listening, HotSpot. KD9GCX, listening, HotSpot. KU6P, listening, HotSpot. KE0KEY, listening, HotSpot. KD4CMK, listening, HotSpot. N4MFJ ...
- Repeater Detail for REF030 - DSTAR Users**  
D-StarUsers.org Your Source for D-Star Digital Amateur Radio Information!  
**KO4WBM**, 05/03/24 07:26:33 UTC, REF030 Dongle User DVD. WA4CQZ, 05/03/24 07:26:07 UTC, REF030 Dongle User DVD. W4BWT, 05/03/24 07:26:07 UTC, REF030 ...

# CVEs and Ham Radio

Common Vulnerabilities and Exposures (CVE) is a list of publicly known computer security flaws. CVEs are assigned a unique ID number, and are used to help IT professionals prioritize and address vulnerabilities

Here are some CVEs related to amateur radio:

- **CVE-2022-1199:** A flaw in the Linux kernel that allows an attacker to crash the kernel by simulating amateur radio
- **CVE-2022-1204:** A use-after-free flaw in the Linux kernel's Amateur Radio AX.25
- **CVE-2022-1205:** A NULL pointer dereference flaw in the Linux kernel's Amateur Radio AX.25 protocol that allows a local user to crash the system

# Relatively safe

- Attackers do not want to:
  - send QSL cards on your behalf.
  - update your log.
  - use your radio to transmit.
- Make sure:
  - Using an OS that is patched regularly.
  - Remote Access into your home is secured (RDP is inherently insecure).
  - You don't download "malicious" free software.
  - Separate computers/tablets if you can.
- SDRs are IoT Devices (they need protection)

Thank You