



Cybersecurity & Service:

Protecting Ourselves, Our businesses, and Our
Communities Online



About the Presenter

Joshuah Williams, CISSP

Senior Threat Hunter | Cybersecurity Leader | Military Veteran



- 19 years of military service in cyber operations and information security
- Leads a team of threat hunters focused on detecting and investigating advanced cyber threats
- Master's Degree candidate in Information Security Engineering
- Certified Information Systems Security Professional (CISSP)
- Multiple professional certifications in:
 - Digital Forensics
 - Incident Response
 - Threat Hunting
 - Network Security Monitoring
 - Security Leadership
- Frequent instructor and presenter on cybersecurity awareness and cyber defense topics



Why Cybersecurity Matters

- We all use the internet daily: shopping, banking, email, social media
- Cybercriminals don't discriminate — they target everyone
- Service Above Self also applies online
- Rotarians are trusted leaders, business owners, managers, and volunteers



Common Online Threats (2026)

Phishing Emails &
Texts – fake urgent
messages

Phone Scams –
'tech support' or
'grandparent'
scams

Romance Scams –
fake online
relationships
asking for money

Shopping Scams –
fake online stores
or deals too good
to be true

Identity Theft –
stealing personal
info for fraud

AI Voice Cloning &
Deep Fakes



Phishing: (Still) The #1 Threat

Urgent or *threatening* tone
("Your account will be locked!")

Unknown links or attachments

Credential requests

Golden Rule:

Don't click suspicious links: verify directly



Phone Scams

Tech Support Scam:

- Someone calls claiming your computer has a virus

Government Scam:

- Fake IRS, Medicare, or Social Security threats

Grandparent Scam:

- “Hi Grandma, I’m in trouble and need money!”

Action:

- **Hang up.** Call back using the official number, not the one provided



Romance Scams



Criminals build trust online through dating apps or social media



Red Flags:

- Move too fast emotionally
- Ask for money for emergencies or travel
- Refuse to meet in person or video chat



Tip: Never send money or gift cards to someone you haven't met in person



Shopping, Investment, & Giveaway Scams



Fake websites with 'too good to be true' deals



Fake charity appeals
(after disasters or holidays)



Giveaway or lottery scams
("You've won!")



- Check the website URL carefully
- Buy only from trusted retailers
- Never pay with gift cards or wire transfers



Social Media Safety

Be mindful of oversharing personal details (birthday, address, vacations)

Criminals use info for password guesses or scams

Beware of quizzes ('What was your first car?') — they often ask password hint questions

Privacy settings: Review who can see your posts



AI Voice & Deepfake Scams



AI Voice & Deepfake Scams



AI Voice & Deepfake Scams

Artificial Intelligence can now generate:

- Realistic voices
- Phone calls
- Video messages
- Emails and text messages

Creating a convincing voice clone may require less than 30 seconds of audio



Spotting Red Flags



Requests for
gift cards,
wire
transfers, or
crypto

Requests for
secrecy
("Don't tell
your family")

High-pressure
tactics
("Act now!")

Trust your gut
feeling

Tip: If it elicits an emotional response, **pause** and **verify** the message

Passwords & Accounts

- Change default passwords
- Use strong, unique passwords for each account
- Consider a password manager
 - LastPass
 - KeyPass
 - 1Password
 - BitWarden
 - Web Browser (Chrome, Edge ...)
- Enable two-factor (2FA) or multi-factor authentication (MFA) whenever possible
- DON'T
 - Use your name or email address
 - Choose common or easy to guess combinations (password, 12345, abcde)
 - Use personal info (birthday, anniversary)

Password Complexity

Rotary123

RotaryClub2026!

ServiceAboveSelf!2026

PurpleMooseDances@Sunrise



Protecting Your Devices

- Keep software, browsers, and apps up to date
- Install antivirus/security tools (many built-in already)
- Lock your phone & computer with a PIN or fingerprint
- Back up important files (cloud or external drive)



Protecting Your Business



Patches & Updates

Backup & Recovery

Cyber Awareness
Training

Incident Reporting



Protecting Yourself & Loved Ones

Talk openly with family and friends about scams

Help elderly relatives spot suspicious calls/emails

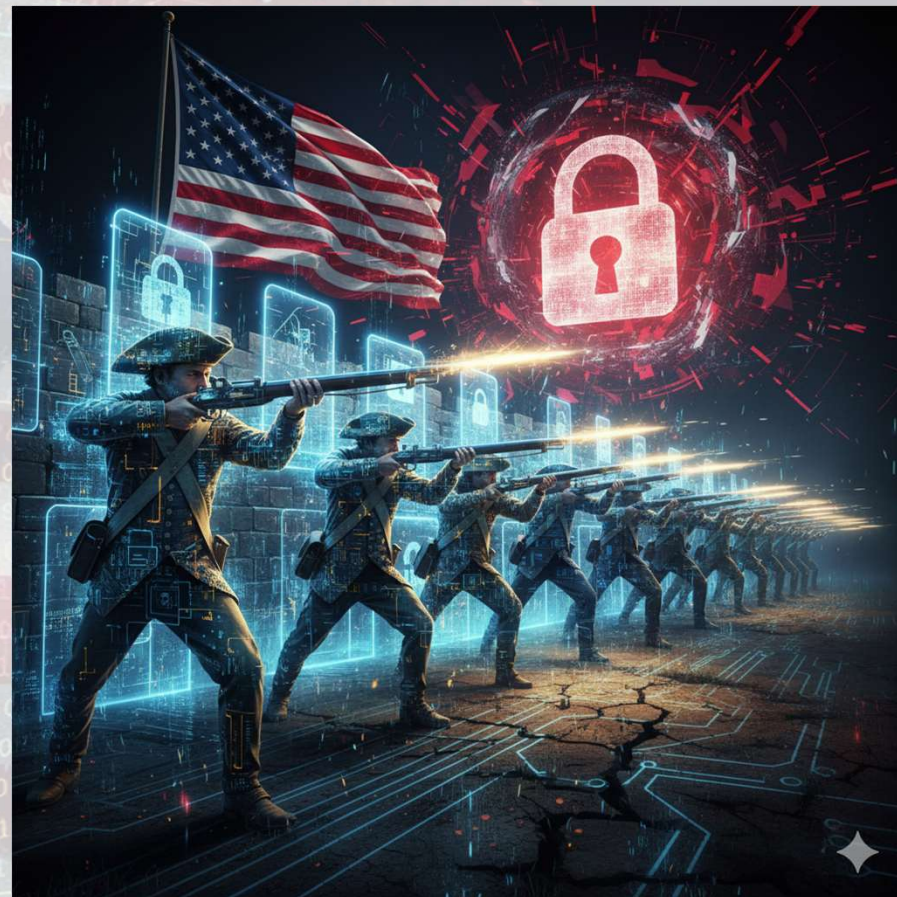
Report scams to:

- [FTC.gov/complaint](https://www.ftc.gov/complaint)
- AARP Fraud Watch Network
- Local law enforcement if money was lost



Summary

- ✓ Strong, unique passwords
- ✓ Multi-Factor Authentication (MFA)
- ✓ Don't click links in unexpected emails/texts
- ✓ Use security updates & backups
- ✓ Be skeptical, verify calls & requests directly
- ✓ When in doubt — **Pause, Verify, Protect**



Resources

FTC Scam Alerts:

www.consumer.ftc.gov/features/scam-alerts

AARP Fraud Watch:

www.aarp.org/money/scams-fraud/

IdentityTheft.gov:

www.identitytheft.gov

Local banks, credit unions, and senior centers often offer free workshops

Have I Been Pwned Password checker:

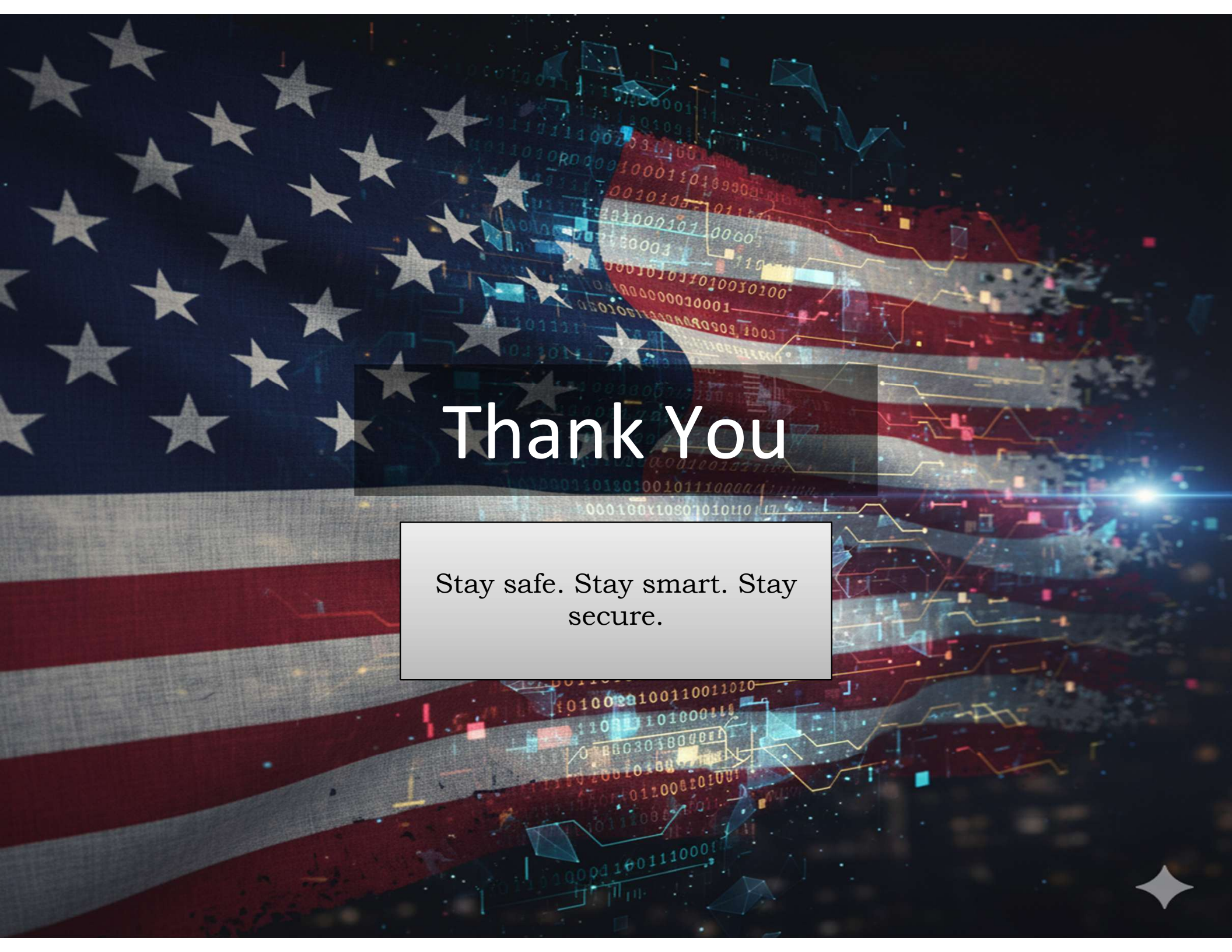
haveibeenpwned.com



Q & A



Questions?



Thank You

Stay safe. Stay smart. Stay
secure.

