Information Security Awareness

MPAFUG – January 2026 Presented by:
Bill Heck, Optiv Security

Purpose: To help individuals recognize common scams, protect personal information, and adopt practical security habits for everyday life.

1. Introduction

● Why scams are increasing
● How technology (AI, spoofing, automation) makes scams harder to detect
● Importance of awareness and verification

2. Understanding Scams: How to Identify One

Common Scam Characteristics

● Impersonation ○ Pretending to be a trusted organization (government, banks, utilities, charities)
○ Use of real names, logos, and spoofed phone numbers or emails

● Problems or Prizes ○ Claims you owe money, your account is compromised, or your device is infected
○ Notifications of winnings or refunds that require action

● Urgency and Pressure ○ Threats of arrest, fines, account suspension, or loss of services
○ Demands to act immediately without time to think or verify

● Specific Payment Methods ○ Requests for gift cards, wire transfers, cryptocurrency, or payment apps
○ Fake checks with instructions to send money back

3. SMS / Text Message Scams

Why Text Scams Are Effective

● People tend to trust text messages
● Short format encourages quick reactions

Common Examples

● Bank or account alerts
● Package delivery issues
● Password reset or security warnings

Warning Signs

● Unexpected messages
● Suspicious links
● Requests for personal or financial information

4. Password Security

Common Problems

● Weak passwords
● Reusing passwords across multiple sites
● Short passwords that are easy to guess or crack

Best Practices

● Use a **unique password** for each important account
● Create passwords that are **at least 12 characters long**
● Use passphrases instead of single words
● Avoid personal information in passwords

5. Password Managers

What Password Managers Do

● Store passwords securely
● Generate strong, random passwords
● Auto-fill login credentials
● Remind you to update passwords

Examples

● KeePass / KeePassXC
● Bitwarden
● 1Password
● Keeper
● NordPass
● RoboForm
● Apple Passwords (macOS)

Best Practices

● Protect with a strong master password
● Enable multi-factor authentication on the manager itself

6. Multi-Factor Authentication (MFA)

What Is MFA?

Using two or more verification factors:

- Something you know (password)
- Something you have (phone, token)
- Something you are (fingerprint, face scan)

Why MFA Matters

- Prevents account access even if a password is stolen
- One of the most effective defenses against phishing

Recommendation

- Enable MFA wherever it is available
- Prioritize email, banking, and financial accounts

7. Artificial Intelligence & Voice Cloning Scams

Emerging Threats

- AI-generated voices that mimic real people
- Fake emergency calls from “family members”
- “Yes” scams that capture voice confirmation

Key Risk

- Voice alone can no longer be trusted as proof of identity

Protection Tips

- Verify emergencies independently
- Call back using a known phone number
- Establish family verification phrases

8. Delivery Scams

How Delivery Scams Work

- Messages reference packages you didn’t order or aren’t tracking
- Links lead to fake websites designed to steal information

How to Protect Yourself

- Keep track of expected deliveries
- Know delivery companies’ communication policies
- Never share personal or payment information from unsolicited messages
- Verify through official company websites or phone numbers

9. 2026 Security New Year’s Resolutions

Smart Online Behavior

- Be cautious with unsolicited emails and messages
- Never send money to strangers
- Research sellers before making online purchases
- Think before clicking links or opening attachments

Strong Security Habits

- Use strong, unique passwords
- Enable two-factor authentication
- Review bank and credit card statements regularly
- Use privacy settings on social media
- Stay informed about new scam techniques

10. Trivia & Scam Recognition Practice

- Impersonation scams
- Online purchase scams
- Phishing emails and texts
- Investment scams
- Real-world decision-making scenarios

11. Key Takeaways

- Scammers rely on **urgency, fear, and trust**
- Technology makes scams more convincing—but awareness stops them
- Verification is your strongest defense
- Strong passwords and MFA significantly reduce risk

Contact Information

Bill Heck bill.heck71@gmail.com