National Cyber Security Awareness Month
Week 1 - Malware

National Cyber Security Awareness Month

Do Your Part. #BeCyberSmart

Protect Yourself

Protect the Mission

Digitally adept Airmen keep personal and mission information protected from the enemy!

National Cyber Security Awareness Month

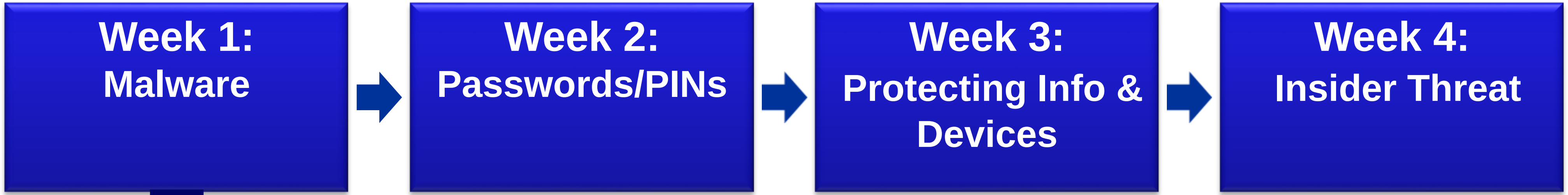
“From the flight line to the front line, from the cockpit to the clinic, we will develop leaders of character with a natural bias for action and a competitive, curious and innovative mindset. We will grow Airmen who are resilient, multi-capable and digitally adept—instinctively exploiting advances in data, computing and information technologies—and armed with the specific skills to deliver into the future.”

- Gen. Jacqueline Van Ovost, AMC Commander

Gen. Jacqueline Van Ovost

National Cyber Security Awareness Month

Each week in October is dedicated to a specific Air Force cyber topic



Week 1: Malware

Week 2: Passwords/PINs

Week 3: Protecting Info & Devices

Week 4: Insider Threat

Malware, why do I care?

How do I identify it?

How can I remove it?

Malware, Why Do I Care?

- Malware infected systems can jeopardize our mobility mission and our Airmen
- We must do everything we can to ensure our aircraft are mission ready
- Malware as a cyber weapor
  - Recent examples:
    - WannaCry ransomware
    - Remote Access Trojan

Key personnel are often targeted and unknowingly spread malware to other systems

Malware Infects Aircraft

Aircraft Cyber Risk is a Real Concern

"Security researchers have already shown the world that commercial jets are vulnerable to hacking, and just last month Washington issued a directive ordering federal agencies to 'defend the skies' against cyber attacks. Concerns over the security of connected cars and aircraft have been expressed for years - like the Jeep hack that demonstrated how software can be manipulated to ignore driver inputs."

Source: George Avetisov Former Forbes Contributor

Photocredit: Airforcetimes.com/Stephen Losey

Photocredit: Getty

Air Mobility Warriors – Projecting Decisive Strength and Delivering Hope… Always!

Malware Progression & Identification

AF Member Opens Phishing / Malware Email

Malware Infected System

Flight Information Compromised

Aircraft Grounded

<u>Possible Symptoms:</u>

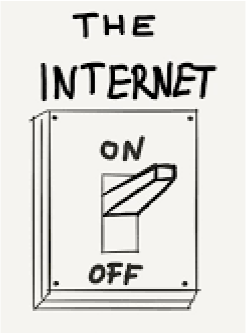
Unexpected Warning Messages
PC Failure
Slow Internet
Colleagues Reporting Suspicious messages from you that you did not send
Pop-up Messages
Unusual Icons Appearing On Desktop

<u>Possible Malware Outcomes:</u>

Data Theft/Alteration
Mission Delay
Aircraft Grounded

Malware – What To Do

If your personal system is compromised:



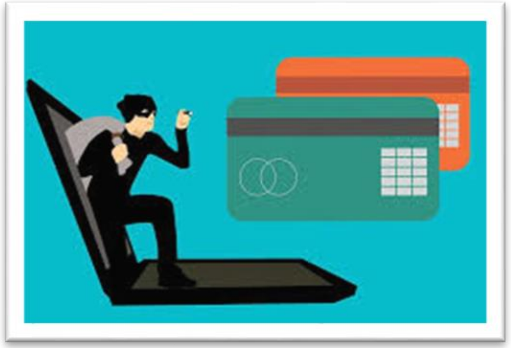
1. Disconnect from the internet

3. Scan Your Device

Free McAfee for home use

2. Close accounts or modify account security settings and passwords

4. Monitor your credit reports



Malware – What To Do

If your Government system is compromised:

1. Immediately disconnect the system from the network. Do not power off, do not logoff.
2. Run a custom McAfee virus scan, scan for threats, allow the scan to complete
3. Right click on the Start Menu button on the Windows Desktop select “File Explorer”
   - In the file Explorer window right click on the drive or partition you want to scan for threats
   - In the pop up window select Scan for threats
   - Allow the scan to complete
4. Report the issue to the unit **Cybersecurity Liaison**
5. Ensure no one uses the system until the threat has been removed/remediated
6. Record all information regarding the incident

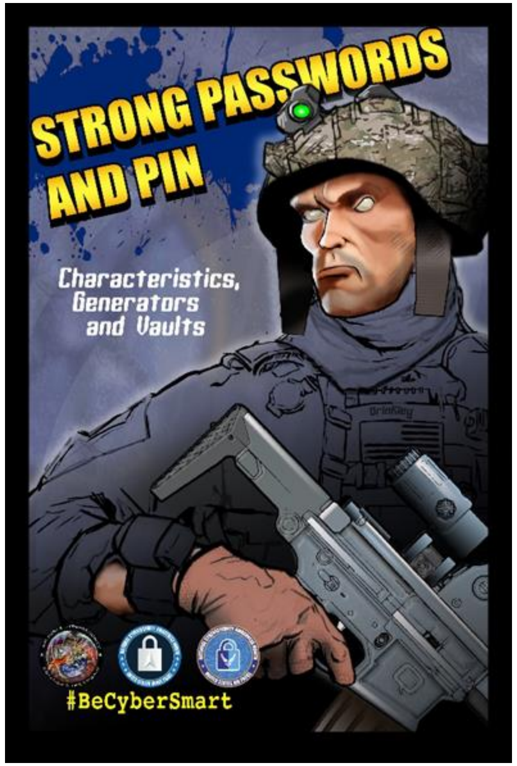
Use your locally-developed Computer Emergency Quick Response Checklist

National Cyber Security Awareness Month

Stay Tuned!!

<u>Week 2 Theme:</u>

Passwords and PINs



For more information, please contact your Wing Cybersecurity Office
or
MAJCOM Cybersecurity Office at: AMC.Cybersecurity@us.af.mil