

# CYBER AWARENESS TRAINING

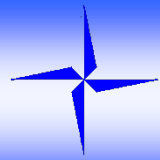


NATO

OTAN











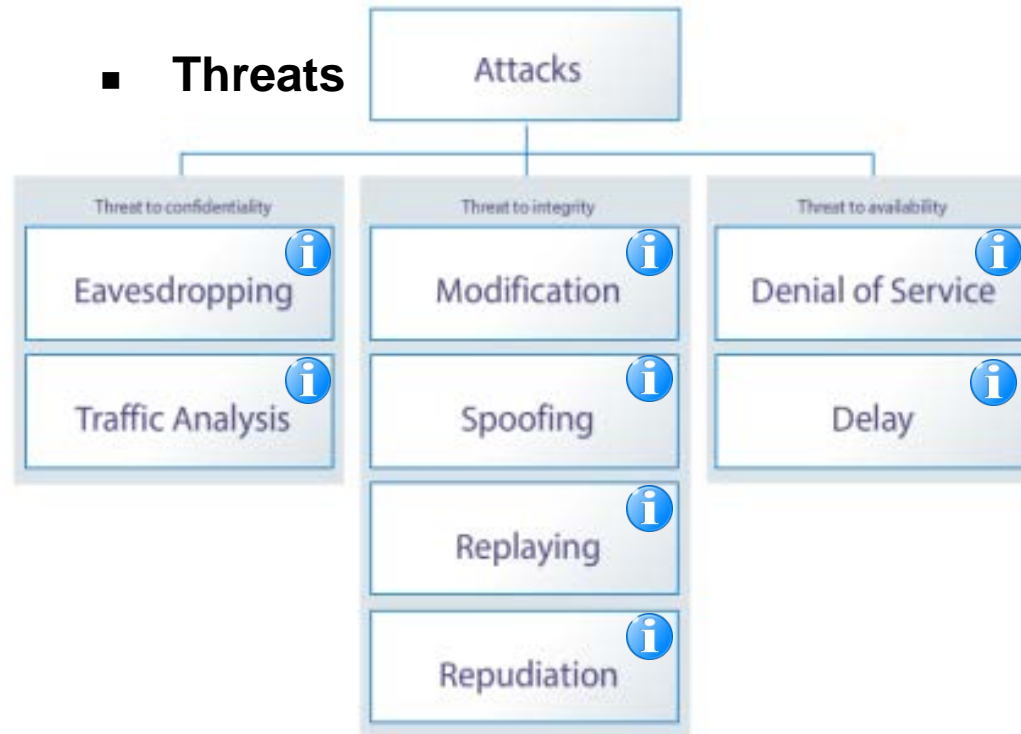
# Types of threats and attackers



- **Attackers** 
  - Cybercrime 
  - Cyber warfare 
  - Hacktivism 
  - Cyber terrorism 
  - Unintentional insiders 













- **Threats**





# MALWARE

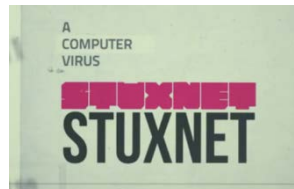


- **MALWARE**, 
  - Trojan horse 
  - Worms 
  - Ransomware 
  - Viruses 
  - Adware 
  - Spyware 
  - Rootkit 
  - Bug 
  - Bots 



- **Example of Malware**

Click on the video of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) cyber training





# Antivirus



## ■ How it works



### Anomaly detection

- Uses a model of usual behaviour of a system.
- Statistical characterisation of what is usual.
- Tries to detect deviations from the usual behaviour.
- Unusual behaviour is classified as bad.

### Misuse (signature-based) detection

- Compares actions and states with known sequences of actions and states while under attack.
- Can only detect known attacks.



### Specification-based detection

- Classifies states and actions that violate the specification as bad.
- Does not play a big role today.

### White listing

- Some vendors generate and maintain a list of signatures of 'known good' applications and compare them against the one found on the systems.



## ■ Recommendations



Prefer a complete security suite that matches your performance requirements and required security level.





Use a regularly updated browser with integrated protections or an A/V software with web-protection.



# Passwords



## ■ Type of attacks

- Brute force, 
- Dictionary, 

### TOP 20 MOST COMMON PASSWORDS

*(as a percentage of all passwords)*

1. 123456	4.1%	11. login	0.2%
2. password	1.3%	12. welcome	0.2%
3. 12345	0.8%	13. loveme	0.2%
4. 1234	0.6%	14. hottie	0.2%
5. football	0.3%	15. abc123	0.2%
6. qwerty	0.3%	16. 121212	0.2%
7. 1234567890	0.3%	17. 123654789	0.2%
8. 1234567	0.3%	18. flower	0.2%
9. princess	0.3%	19. passw0rd	0.2%
10. solo	0.2%	20. dragon	0.1%

  
**A STRONG  
PASSWORD  
IS  
A GOOD  
PASSWORD**

## ■ Password strength

- 9 characters including : 1 capital letter, 1 number, 1 special character

### strong password idea generator

**2** word ideas {  
• animal • color • team • car model • celebrity name  
• food • game • hobby • title (movie, book, show, etc.)  
+  
**1** number idea {  
• year • statistic (e.g., RBI, GDP) • lucky number  
• scientific constant • random number • age  
+  
**1** capital letter {  
• or more • in a rAnDom spot



## ■ Re-use password + changing password



K3l(Y\_faCe



K3l(Y\_ma1l



K3l(Y\_tw33t






K3l(Y\_ty6e



# Identity theft and emails



## ■ Dangers

- Phishing, 
- Spear phishing, 
- Social engineering, 



## ■ Video fake URL

## ■ Example of phishing email

**Subject:** \*\*\*\*\*SPAM\*\*\*\*\* PayPal Notification [REF ID: X87HF]  
**From:** support@securitynet.com <support@securitynet.com>  
**Date:** 10/14/2009 07:23 PM  
**To:** undisclosed-recipients;;

Dear PP member,  
You have (1) new security message from Security Center.  
Please click on the link below and update your profile.

<http://www.paypal.com.cmd.ppiusf.com/pp/us/login.htm>

**Subject** – Distributed as a spam e-mail

**From** – The sender tries to disguise as some security company in order to look important

**To** – Harvested recipient addresses

**Body** – The included link contains paypal.com in the host address part, but does not actually point to any site related to PayPal. When the user is visiting the website, he is asked to input his user credentials or identity information.

## Example of phishing website








# Mobile devices



## ■ Risks

- Data Leakage 
- Unsecured Wi-Fi
- Network Spoofing
- Phishing Attacks
- Spyware
- Broken Cryptography
- Improper Session Handling

## ■ Vulnerabilities

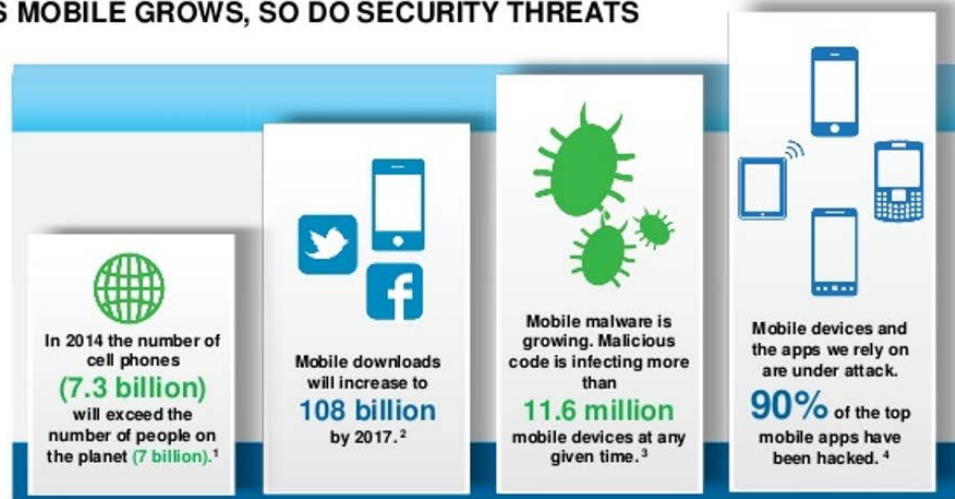
- Malware
- Device vulnerabilities
- Data leaks
- Physical protection

## ■ Best practices

- Regularly update the operating system and apps
- Use relevant built-in security features
- Minimize location access
- Avoid connecting to unsecured Wi-Fi networks
- Download apps from trusted sources
- Know the risks of jailbreaking/rooting
- Be wary of unsolicited calls or messages
- Set automatic locks on mobile devices
- Limit the personal information given to apps and websites
- Manage what is shared online
- Be aware of the nature of your conversation and your surroundings

## THE STATE OF MOBILE SECURITY

AS MOBILE GROWS, SO DO SECURITY THREATS







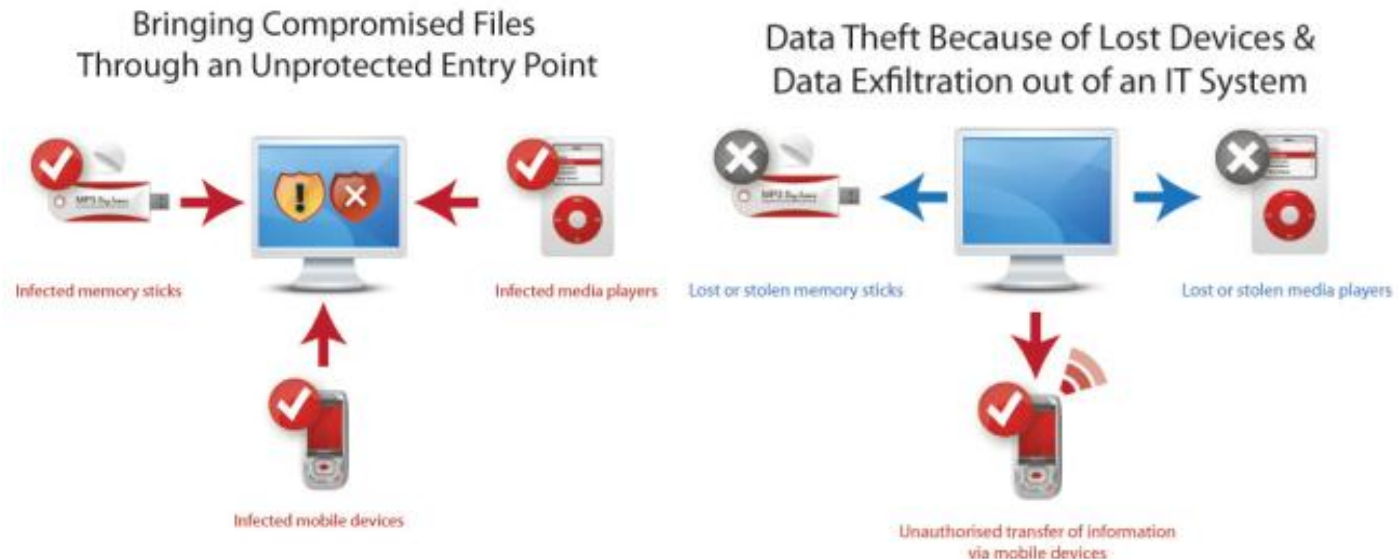
# Removable media



- **Type**



- **Risks**



- **Recommendations**






- Every division within HQ MARCOM has a **Divisional File Transfer Secretary** authorized to transfer data between NS/NU networks (HQTM 006/14)



# Social media







## ■ Dangers

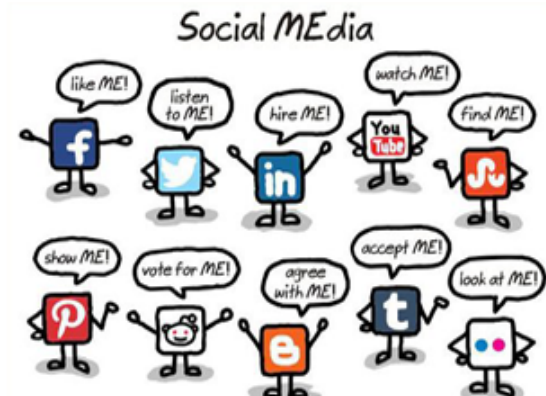
- Defeating passwords 
- Social engineering 
- Identity theft
- Exploitation by Foreign Intelligence Services 
- Physical interception 
- Blackmail 



## ■ Recommendations

- Arranging privacy settings to protect a personal social media profile, noting that individual account settings can affect anyone that has links to that account.
- Speaking to family and friends about what they post and 'tag' to their social media accounts.
- Considering what is uploaded, whether it is an image or information, and who may access it.
- Awareness of geo-data attached to uploaded content.
- Considering whether there is a need to identify as a military member, and what other personal and sensitive information is attached to NATO member's social media profile.

- **Personal Security Online : navy** 
- **Personal Security Online : friends and family** 
- **Personal Security Online : defence civilians** 
- **Personal Security Online : army** 





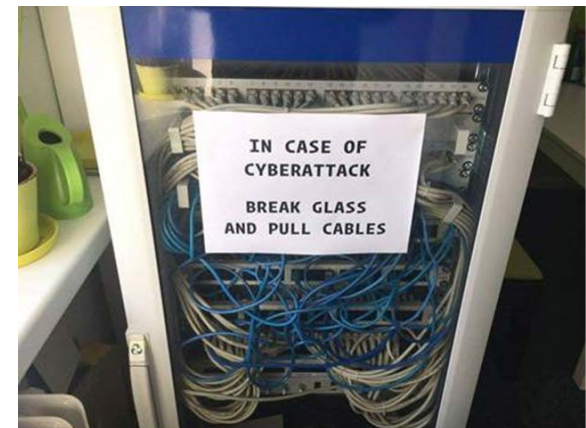
# MARCOM SOI 409.02

## Mobile phones and connected devices



### ■ POLICIES FOR THE USE OF MOBILE COMMUNICATION DEVICES (MCD)

- No MCD shall be introduced into Atlantic Building
- All MCD will be stored in the dedicated lockers at corridor. Such phones will be turned off.
- All MCD, regardless of the ownership, will only be used for the conveyance of publicly release and non-sensitive NATO UNCLASSIFIED information.
- In cases when an official has NATO approved secure voice capability, the classification of the information exchange may be up to NATO SECRET, if all other rules and regulations (e.g. COMSEC doctrine for device) are observed.
- It is chairperson's responsibility to preface all proceedings held in the MARCOM conference rooms with a verbal reminder to remove MCD from the building.







# Types of malware

## Question 1/3



1. Why is even a very strong password useless if your system is infected with malware?

- ☐ It isn't. Strong passwords are secure and malware does not change that.
- ☐ Malware can log all my keystrokes and record my passwords, no matter how strong they might be.

>>





# Types of malware

## Question 2/3



2. If all your software is always updated immediately, you are safe from malware infections because there are no known exploitable bugs in your software.

☐ True

☐ False





# Types of malware

## Question 3/3



3. Browsing with a smartphone is always safe, as long as you never download suspicious files.



True



False







# Types of threats and attackers

## Question 1/3



1. The security building block "encryption" is important for which of the security goals?

- ☐ Availability
- ☐ Integrity
- ☐ Confidentiality





# Types of threats and attackers

## Answer



1. The security building block "encryption" is important for which of the security goals?

- ☒ Availability
- ☐ Integrity
- ☐ Confidentiality



**FALSE**



Previous



# Types of threats and attackers

## Answer



1. The security building block "encryption" is important for which of the security goals?

- ☐ Availability
- ☒ Integrity
- ☐ Confidentiality

>>



**FALSE**



Previous





# Types of threats and attackers

## Answer



1. The security building block "encryption" is important for which of the security goals?

- ☐ Availability
- ☐ Integrity
- ☒ Confidentiality

>>



TRUE



Next



# Types of threats and attackers

## Question 2/3



2. DDoS attacks are performed by...

- ☐ sending bogus data to trigger crashes.
- ☐ sending a lot of data with a network of machines.
- ☐ using exploits to compromise the remote system.

>>





# Types of threats and attackers

## Answer



2. DDoS attacks are performed by...

- ☒ sending bogus data to trigger crashes.
- ☐ sending a lot of data with a network of machines.
- ☐ using exploits to compromise the remote system.



**FALSE**



Previous



# Types of threats and attackers

## Answer



2. DDoS attacks are performed by...

- ☐ sending bogus data to trigger crashes.
- ☒ sending a lot of data with a network of machines.
- ☐ using exploits to compromise the remote system.



TRUE



Next



# Types of threats and attackers

## Answer



2. DDoS attacks are performed by...

- ☐ sending bogus data to trigger crashes.
- ☐ sending a lot of data with a network of machines.
- ☒ using exploits to compromise the remote system.



**FALSE**



Previous





# Types of threats and attackers

## Questions 3/3



3. Which attacker type are home users mostly threatened by?

- ☒ Individual criminals and organized crime
- ☐ Hacktivists
- ☐ Military personnel

>>





# Types of threats and attackers

## Answer



3. Which attacker type are home users mostly threatened by?

- ☒ Individual criminals and organized crime
- ☐ Hacktivists
- ☐ Military personnel

>>



TRUE



Next



# Types of threats and attackers

## Answer



3. Which attacker type are home users mostly threatened by?

- ☐ Individual criminals and organized crime
- ☒ Hacktivists
- ☐ Military personnel

>>



**FALSE**



Previous



# Types of threats and attackers

## Answer



3. Which attacker type are home users mostly threatened by?

- ☐ Individual criminals and organized crime
- ☐ Hacktivists
- ☒ Military personnel

>>



**FALSE**



Previous



# Antivirus

## Question 1/2



1. Is it possible to get a computer virus from an email if you don't open any attachments?

- ☐ Yes, if your system software isn't properly updated.
- ☐ No, the only way to get a virus from email is to open an infected attachment.

>>







# Antivirus Answer



1. Is it possible to get a computer virus from an email if you don't open any attachments?

- ☒ Yes, if your system software isn't properly updated.
- ☐ No, the only way to get a virus from email is to open an infected attachment.

>>



TRUE



Next



# Antivirus Answer



1. Is it possible to get a computer virus from an email if you don't open any attachments?

- ☐ Yes, if your system software isn't properly updated.
- ☒ No, the only way to get a virus from email is to open an infected attachment.

>>



**FALSE**



Previous



# Antivirus

## Question 2/2



2. When using a good A/V tool, software system updates are not that important.

☐ True

☐ False

>>





# Antivirus Answer



2. When using a good A/V tool, software system updates are not that important.

☒ True

☐ False

>>



**FALSE**



Previous



# Antivirus Answer



2. When using a good A/V tool, software system updates are not that important.

☐ True

☒ False

>>



TRUE



Next





# Passwords

## Question 1/2



1. A good password contains letters, numbers and special characters.

☒ True

☐ False





# Passwords Answer



1. A good password contains letters, numbers and special characters.

☒ True

☐ False



TRUE



Next



# Passwords Answer



1. A good password contains letters, numbers and special characters.

☐ True

☒ False



**FALSE**



Previous



# Passwords

## Question 2/2



2. Using two-factor authentication is better than strong password.

☒ True

☐ False

>>





# Passwords Answer



2. Using two-factor authentication is better than strong password.

☒ True

☐ False

>>



TRUE



Next





# Passwords Answer



2. Using two-factor authentication is better than strong password.

☐ True

☒ False



**FALSE**



Previous



# Identity theft and emails

## Question 1/3



1. Always updating all your software as well as running an A/V tool will effectively protect you from phishing.

☒ True

☐ False





# Identity theft and emails

## Answer



1. Always updating all your software as well as running an A/V tool will effectively protect you from phishing.

☒ True

☐ False



**FALSE**



Previous



# Identity theft and emails

## Answer



1. Always updating all your software as well as running an A/V tool will effectively protect you from phishing.

☐ True

☒ False



TRUE



Next



# Identity theft and emails

## Question 2/3



3. If you receive an email from your bank, always click on the link provided in the email.

☒ True

☐ False





# Identity theft and emails

## Answer



3. If you receive an email from your bank, always click on the link provided in the email.

☒ True

☐ False



**FALSE**



Previous



# Identity theft and emails

## Answer



3. If you receive an email from your bank, always click on the link provided in the email.

☐ True

☒ False



TRUE



Next



# Identity theft and emails

## Question 3/3



1. A system administrator calls you on the phone and asks for your help. For security reasons, he needs to check if the passwords of all employees are strong enough and therefore asks you to tell him your password. What do you do?

- ☒ I get suspicious and do not tell him anything. A real system administrator would never ask for my password.
- ☐ I tell him the password because it is important that all passwords are strong enough.







# Identity theft and emails

## Answer



1. A system administrator calls you on the phone and asks for your help. For security reasons, he needs to check if the passwords of all employees are strong enough and therefore asks you to tell him your password. What do you do?

- ☒ I get suspicious and do not tell him anything. A real system administrator would never ask for my password.
- ☐ I tell him the password because it is important that all passwords are strong enough.



TRUE



Next



# Identity theft and emails

## Answer



1. A system administrator calls you on the phone and asks for your help. For security reasons, he needs to check if the passwords of all employees are strong enough and therefore asks you to tell him your password. What do you do?

- ☐ I get suspicious and do not tell him anything. A real system administrator would never ask for my password.
- ☒ I tell him the password because it is important that all passwords are strong enough.



**FALSE**



Previous



# Mobile devices

## Question 1/2



1. What is the relevant problem with posting location data from an MD to a social network regularly?

- ☒ Attackers might use the knowledge about my location to predict my schedule and choose attack times.
- ☐ My friends can easily organize a surprise party for me at an unwanted venue.
- ☐ The police can use the location data to accurately assign speeding tickets.





# Mobile devices Answer



1. What is the relevant problem with posting location data from an MD to a social network regularly?

- ☒ Attackers might use the knowledge about my location to predict my schedule and choose attack times.
- ☐ My friends can easily organize a surprise party for me at an unwanted venue.
- ☐ The police can use the location data to accurately assign speeding tickets.



TRUE



Next



# Mobile devices Answer



1. What is the relevant problem with posting location data from an MD to a social network regularly?

- ☐ Attackers might use the knowledge about my location to predict my schedule and choose attack times.
- ☒ My friends can easily organize a surprise party for me at an unwanted venue.
- ☐ The police can use the location data to accurately assign speeding tickets.



**FALSE**



Previous



# Mobile devices Answer



1. What is the relevant problem with posting location data from an MD to a social network regularly?

- ☐ Attackers might use the knowledge about my location to predict my schedule and choose attack times.
- ☐ My friends can easily organize a surprise party for me at an unwanted venue.
- ☒ The police can use the location data to accurately assign speeding tickets.



**FALSE**



Previous



# Mobile device Question 2/2



There is no danger if I plug my MD on my desktop/laptop.

☐ True

☐ False





# Mobile device Answer



There is no danger if I plug my MD on my desktop/laptop.

☒ True

☐ False



**FALSE**



Previous





# Mobile device Answer



There is no danger if I plug my MD on my desktop/laptop.

☐ True

☒ False



TRUE



Next



# Removable media

## Question 1/2



2. You regularly scan your removable media (like USB sticks) for viruses. It is therefore safe to use those devices on all systems.

☒ True

☐ False





# Removable media Answer



2. You regularly scan your removable media (like USB sticks) for viruses. It is therefore safe to use those devices on all systems.

☒ True

☐ False



**FALSE**



Previous



# Removable media Answer



2. You regularly scan your removable media (like USB sticks) for viruses. It is therefore safe to use those devices on all systems.

☐ True

☒ False



TRUE



Next



# Removable media

## Question 2/2



3. You find a USB stick in your company's parking lot. What do you do?

☐ I plug it into my computer but scan for viruses before I open any files.

☐ I do not plug it in but ask my system administrator if it is safe to do so.





# Removable media Answer



3. You find a USB stick in your company's parking lot. What do you do?

- ☒ I plug it into my computer but scan for viruses before I open any files.
- ☐ I do not plug it in but ask my system administrator if it is safe to do so.



**FALSE**



Previous



# Removable media Answer



3. You find a USB stick in your company's parking lot. What do you do?

- ☐ I plug it into my computer but scan for viruses before I open any files.
- ☒ I do not plug it in but ask my system administrator if it is safe to do so.



TRUE



Next



**Please submit your completion and add your full name, rank and division in the email body**

**“certificate will be sent by email once received by N6 CYBER”**



**Click here to submit your completion**