Security Awareness Training Campaign

Alice Mace

Cybersecurity, Bellevue University

CYBR 520: Human Aspects of Cybersecurity

Professor Karla Carter

May 30, 2022

The Missile Defense Agency Intelligence Directorate will be running a campaign for Cybersecurity Awareness Month. Each week will have a different topic related to cybersecurity and activities to encourage participation and education on concerns and mitigations in that realm. With ever increasing cyber-attacks, it's necessary to educate our organization on the risks and small things that can be done to drastically change the impact of an attack. Current planned topics are as follows:

Week 1: Device security and "Find the Phone" exercise

Week 2: Network security education

Week 3: Spillage awareness

Week 4: Suspicious network activity and clearance requirements

Week 1 emphasizes the security aspects of our personal devices that can be implemented to ensure the security of each employee's information. This also ensures that any work-related information that may be conducted on a personal device is better protected. While all work done on/through personal devices must be unclassified, the compilation of information is always a concern and can lead to operational security issues. The "Find the Phone" exercise is designed to practice situational awareness and bring focus to the risks of personal electronic devices in controlled areas. The inside of the phone case has a sticky note that reads "Always Listening!" followed by a camera, Bluetooth, and WIFI symbol that ties into the Devise security poster. It will be conducted with an empty phone case, pictured in the flyer, and leadership will be well informed of the exercise before it is conducted to avoid any concerns of an unauthorized device being brought into a controlled space. As each person finds the phone case and notifies security, they will be given a small reward and also asked to review and sign acknowledging the Agency's policy of personal electronic devices in controlled areas.

Week 2 focuses on education of network security aspects and highlights that the average user may not be aware of. This not only helps with general user awareness, but it also assists in bridging the gap between users and IT/Security staff on the concerns that the other group is evaluating. Education on these concepts helps to facilitate more clear lines of communication between these groups and helps the users understand the "why" behind several concerns and requirements. This week a crossword puzzle will be sent out to the office and individuals will once again be given a small reward for correctly completing it. It includes network security terms, security measures, and hardware that is key to ensure the security of a system.

Week 3 brings the persistent concern of information spillage to the foreground and highlights that it is not something to be taken lightly. Making personnel more aware of an issue and the importance of reporting it immediately, if/when it occurs, allows for more time to address the issues before it gets too far out of hand. One of the most prominent violations of spillage is people not being cognizant of what system they are working on and unintentionally putting classified information in an email. Reminders, such as the Spillage poster, to be aware of networks and the importance of information security help reduce this risk. This week is also accompanied by a word search that will be emailed out and includes terms associated with security and spillage events.

Week 4 follows suit with a similar aspect of the importance to report issues, but focuses in depth on reporting suspicious network and personnel activity. Phishing emails are a constant threat and can be disastrously harmful to a system. Even if a user is not aware that they may have something malicious on their system, we’re encouraging them to report any strange activity they encounter, as that is commonly a sign of malicious code. Also, reminders for personnel to ensure their clearance information is up to date and any reporting requirements are met to maintain their credentials will be covered. While this is not directly related to cybersecurity, it does determine their ability to conduct their responsibilities dealing with classified information and provides a good baseline of information to look out for regarding potential insider threats. More often than not, insider threat behavior can directly correlate to events that must be reported to maintain a clearance and all individuals in the Missile Defense Agency Intelligence Directorate are required to hold a clearance for employment.

Each of these weeks during Cybersecurity Awareness Month provides an opportunity to better educate and prepare personnel against various cyber-attacks and to preemptively counter vulnerabilities. Small adjustments can make a large impact over time or if a large enough group is implementing these controls. It is critical to remain vigilant against cyber-attacks and maintain the security of our nation’s critical information.

MISSILE DEFENSE AGENCY
DEPARTMENT OF DEFENSE

Is your device secure?

When was the last time you checked your personal device security settings?

- Automatic location sharing?
- Granting permissions for app data sharing?
- Connecting to open WiFi networks?
- Smartphone virus scans?
- Aware of smishing?
- Accessible bank information?
- Is Siri always listening?
- Invasive smartphone spyware detection?
- Updated software patches?
- Continuous open sessions?

Talk to the Security team today for more information on securing your personal devices.

FIND THE PHONE

When

Week 1 of Cybersecurity Awareness Month

What To Do

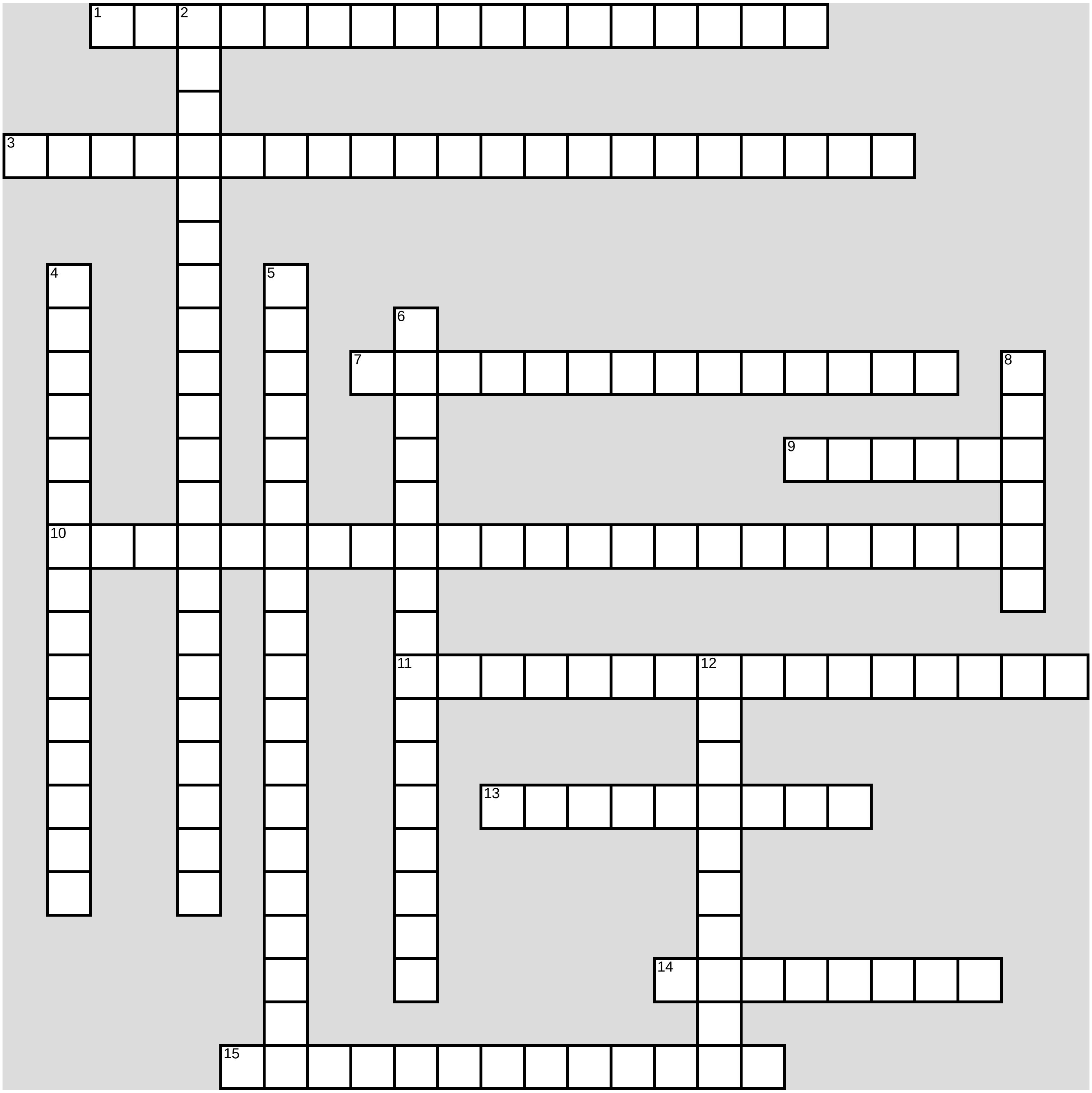
Locate the phone case each day and report to security where it was for a reward

Why

Practice your situational awareness and acknowledge the risk of devices in secure spaces
#alwayslistening

MISSILE DEFENSE AGENCY
DEPARTMENT OF DEFENSE

Network Secuirty



Across

1 An interruption in an authorized user's access to a computer network

3 At least 10 characters, at least 3 uppercase, lowercase, numeric, or special characters

7 Corrects a vulnerability to hacking or viral infection

9 Connects devices to network

10 Aability to make major changes to a system

11 New version of the software product

13 Confidentiality, integrity and availability of data

14 Designed to block unauthorized access while permitting outward communication

15 Fake information is entered into the cache of a domain name server

Down

2 Process of assigning network settings, policies, flows, and controls

4 On-site access to computer and network hardware

5 Ability to monitor and react to computer misuse

6 Focuses on protecting the components of an organization’s network

8 Manages network resources

12 The process of converting information or data into a code

Network Secuirty

		1 D	E	2 N	I	A	L	_	O	F	_	S	E	R	V	I	C	E						
				E																				
				T																				
3 P	A	S	S	W	O	R	D	_	R	E	Q	U	I	R	E	M	E	N	T	S				
				O																				
				R																				
	4 P			K		5 I																		
	H			_		N			6 N															
	Y			C		T		7 S	E	C	U	R	I	T	Y	_	P	A	T	C	H		8 S	
	S			O		R			T														E	
	I			N		U			W									9 R	O	U	T	E	R	
	C			F		S			O														V	
	10 A	D	M	I	N	I	S	T	R	A	T	O	R	_	P	R	I	V	I	L	I	G	E	
	L			G		O			K														R	
	_			U		N			_															
	A			R		_			11 S	O	F	T	W	A	R	12 E	_	U	P	G	R	A	D	E
	C			A		D			E							N								
	C			T		E			C							C								
	E			I		T			U		13 C	I	A	_	T	R	I	A	D					
	S			O		E			R							Y								
	S			N		C			I							P								
						T			T							T								
						I			Y						14 F	I	R	E	W	A	L	L		
						O										O								
					15 D	N	H	_	P	O	I	S	O	N	I	N	G							

Across

1 An interruption in an authorized user's access to a computer network

3 At least 10 characters, at least 3 uppercase, lowercase, numeric, or special characters

7 Corrects a vulnerability to hacking or viral infection

9 Connects devices to network

10 Aability to make major changes to a system

11 New version of the software product

13 Confidentiality, integrity and availability of data

14 Designed to block unauthorized access while permitting outward communication

15 Fake information is entered into the cache of a domain name server

Down

2 Process of assigning network settings, policies, flows, and controls

4 On-site access to computer and network hardware

5 Ability to monitor and react to computer misuse

6 Focuses on protecting the components of an organization’s network

8 Manages network resources

12 The process of converting information or data into a code

Know your networks!

Even one spill is one too many!

Protect your data!

Spillage Awareness

```
                            C
                          K R
                          W G F
                        B M X K W
                        J T P S Y X
                      P K L J L K S G
                    V U W D S Z P S T K
                    Q G A I R C P E U I H
                  L F X U M I U Z J K L L W
                  R Y Y Q X W P Z Z U X Y G I
                P N O R I U B Z J G Y O W D P E
                T C A H X A D E T E C T E F Y R A
              L S Q N G T G A W D J A I D X X Q N W
              L T B U N J S T K C E F N J Y S J O O N
            C J M J M J U A Q E I I A R X X S N T D I A
            Q V R H L O K L Q N S N R S I H O N P L F J G
          J D G J W I E Y K F S W E S V A S I N Y D G T M R
          B F G J C N X N I A L G T H Y B P K F H A O P X W Q
        P I O G I V L P L L I I U Z R Z T G I U X T I Z E T N T
        N I D L I C Q T C L P S H E U A T E G W V A Q A S V S O P
      S O D A R P L R X I E C B P P Z M G T L P U G B S I S I O X T
      O V M O H W A I X S Z M O Z K L L O P Z U P J D U N Y W T U O R
    Y L G N P T T L J R G Q R D K M T X C J P F Q K Z B I G Q Y I V U N
    H I M U A E E I E S D T O Z Q X B Y M A V B Z S P H B F F O I S E N L
  K E E E R L Y P K S S A M U S A T E Y G I A E H I M W V Z N G Z L N B I K
  R N J Y R G Y L U A Y J I Q W U H Z R C H E S I M O R P M O C S T O E N I B
I T Z X V G L O S O P J Y C F J Z I S D Y L M G U E Y X E R U S O P X E S I D C
                            N
                            G
                            H
H A C K E R S W K J A N S W U D J Z Q G O S I Y V I A M K V W T N E D I C N I T
  B F T Q A X U C I W T D K N E T W O R K P W F G P S A Z C R U L X Q I L U Y
  N F F S U K K G O H M D E F T G X L B U J M X F P L C F O T J B X L E A K K
    Z L H O K M X C O E M S W L J M U N I A O C I W B H K A X W R G D C J E
    L S R E S G B Z G J M J X L G X R A M W Q L W Q M L C Z V E E N V Y J L
      L U I N F O R M A T I O N O D P K P D L C A N X C O T V A A O H S W
      N I Q Q B N Z K X D M S Y J X D S O A B Z I H J V D O V I C D R O B
        J A A R R R M B T U O F Y W G Z G A M T S D P Z N W T N H K H D
        E L A U N S E C U R E K S N S E H Q U N A U T H O R I Z E D B S
```

WORD LIST:

BREACH
CLASSIFIED
COMPROMISE
DATA
DETECT

ENVIRONMENT
EXPOSURE
HACKERS
INCIDENT
INFILTRATE

INFORMATION
LEAK
MALICIOUS
NETWORK
REPORT

RISK
SENSITIVE
SPILLAGE
UNAUTHORIZED
UNSECURE

Spillage Awareness

```
                          C
                         K R
                        W G F
                       B M X K W
                      J T P S Y X
                     P K L J L K S G
                    V U W D S Z P S T K
                   Q G A I R C P E U I H
                  L F X U M I U Z J K L L W
                 R Y Y Q X W P Z Z U X Y G I
                P N O R I U B Z J G Y O W D P E
               T C A H X A D E T E C T E F Y R A
              L S Q N G T G A W D J A I D X X Q N W
             L T B U N J S T K C E F N J Y S J O O N
            C J M J M J U A Q E I I A R X X S N T D I A
           Q V R H L O K L Q N S N R S I H O N P L F J G
          J D G J W I E Y K F S W E S V A S I N Y D G T M R
         B F G J C N X N I A L G T H Y B P K F H A O P X W Q
        P I O G I V L P L L I I U Z R Z T G I U X T I Z E T N T
       N I D L I C O T C L P S H E U A T E G W V A Q A S V S O P
      S O D A R P L R X I E C B P P Z M G T L P U G B S I S I O X T
     O V M O H W A I X S Z M O Z K L L O P Z U P J D U N Y W T U O R
    Y L G N P T T L J R G Q R D K M T X C J P F Q K Z B I G Q Y I V U N
   H I M U A E E I E S D T O Z Q X B Y M A V B Z S P H B F F O I S E N L
  K E E E R L Y P K S S A M U S A T E Y G I A E H I M W V Z N G Z L N B I K
 R N J Y R G Y L U A Y J I Q W U H Z R C H E S I M O R P M O C S T O E N I B
I T Z X V G L O S O P J Y C F J Z I S D Y L M G U E Y X E R U S O P X E S I D C
                          N
                          G
                          H
H A C K E R S W K J A N S W U D J Z Q G O S I Y V I A M K V W T N E D I C N I T
  B F T Q A X U C I W T D K N E T W O R K P W F G P S A Z C R U L X Q I L U Y
  N F F S U K K G O H M D E F T G X L B U J M X F P L C F O T J B X L E A K K
   Z L H O K M X C O E M S W L J M U N I A O C I W B H K A X W R G D C J E
   L S R E S G B Z G J M J X L G X R A M W Q L W Q M L C Z V E E N V Y J L
    L U I N F O R M A T I O N O D P K P D L C A N X C O T V A A O H S W
    N I Q Q B N Z K X D M S Y J X D S O A B Z I H J V D O V I C D R O B
     J A A R R R M B T U O F Y W G Z G A M T S D P Z N W T N H K H D
     E L A U N S E C U R E K S N S E H Q U N A U T H O R I Z E D B S
```

WORD LIST:

~~BREACH~~
~~CLASSIFIED~~
~~COMPROMISE~~
~~DATA~~
~~DETECT~~

~~ENVIRONMENT~~
~~EXPOSURE~~
~~HACKERS~~
~~INCIDENT~~
~~INFILTRATE~~

~~INFORMATION~~
~~LEAK~~
~~MALICIOUS~~
~~NETWORK~~
~~REPORT~~

~~RISK~~
~~SENSITIVE~~
~~SPILLAGE~~
~~UNAUTHORIZED~~
~~UNSECURE~~

SUSPICIOUS EMAILS OR NETWORK ACTIVITY?

ALWAYS REPORT!

IT HOTLINE: 450-4350

Help keep out networks safe and secure, don’t click links or questionable attachments!

MISSILE DEFENSE AGENCY
DEPARTMENT OF DEFENSE

Report any suspicious activity and ensure clearance reporting requirements are up to date!

What to Report for your Clearance

Top 10 Reporting Requirements for those holding a DoD Secuirty Clearance

Foreign Travel

Any travel outside the United States must be reported, whither the trip is personal or professional.

Foreign Contacts

Regular contact with any foreign national must be reported. This includes family members and/or dual citizens.

Financial Problems

Serious financial problems must be reported, such as bankruptcy, garnishment of wages, a lien placed on property, or eviction.

Arrests

All arrests must be reported immediately, even if not changed or convicted of any crimes.

Other Legal Involvement

Any legal involvement when sworn under oath or and needing to discuss work matters or if being sued must be reported.

Counseling

Phycological or substance abuse counseling must be reported if directed to seek such counseling. If sought out individually, it need not be reported.

Marital Status

Marriage, divorce, plans to marry, or marriage to a foreign national must be reported. Cohabitants and legal name changes must also be reported.

Media Contacts

Any contact with all forms of media related to your work or organization must be reported.

Pre-Publication Review

If any information is used in a technical document that is being submitted publicly, it must be reviewed if any information included was learned while working with classified information.

Loss or Compromise of Information

Any loss or compromise of sensitive or classified information must be reported immediatly, even if unintentionally disclosed.

See Military.com, DSCA.mil, DODM 5105.21 Volume 3, or your local SSO for additional Information