Arkansas Department of Health

Cybersecurity and Awareness Training

The purpose of this training course is to emphasize the scope and the importance of network and Cybersecurity within the Arkansas Department of Health. This training module will help you to understand the best practices involved in protecting the ADH computer network and vital information from outside intrusion and malicious attacks and to create a culture of Cybersecurity in the workplace. As more duties and records are processed and stored online, cybercriminals are there waiting to take advantage of unsuspecting employees to gain access to valuable departmental information. It is the responsibility of every user in every section to protect our organization's network, systems and data. This can best be done by following the acceptable computer usage policies set forth by the Arkansas Department of Health and by implementing the best practices that are covered in this training module.

In addition to the ADH security policies, HIPAA (Health Insurance Portability and Accountability Act), section 164.308, requires that every organization in the healthcare industry implement a security awareness and training program for all members of its workforce (including management).

Recognizing and combating cybercrime presents a unique challenge. In a world filled with technical jargon and complicated concepts, the average person may feel overwhelmed with the idea of protecting themselves from cybercrime. However, there are quick, easy steps everyone can take – no matter their level of technical expertise – to protect themselves online. The first step in protecting yourself against cybercrime is knowing how to recognize it.

The ADH Computer Access Policy

Before we discuss the various methods of identifying potential cybercrime attacks, we need to review the ADH Computer Usage and Access Policy listed below. This policy appears on your computer's login

screen each time you log on to the ADH network. When you click "OK", you sign an agreement to abide by the terms of the policy each time you use an ADH system.

"*Use of this or any other ADH computer system constitutes consent to monitoring at all times. This is an ADH computer system. All ADH computer systems and related equipment are intended for the communication, transmission, processing and storage of official State Government or other authorized information only. All ADH computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems, including security devices and systems; to prevent unauthorized use and violations of statutes and security regulations; to deter criminal activity; and for other similar purposes. Any user of an ADH computer system should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy.*

If monitoring of this or any other ADH computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this or any other ADH computer system reveals a violation of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of ADH computer systems are subject to appropriate disciplinary action. Use of this or any other ADH computer system constitutes consent to monitoring at all times."

Password Security

Every day we arrive at work, park our vehicles and make the effort to lock our vehicle doors. When we hear the locks click and the alarm report ready, we take comfort in knowing that we have done our part to make sure our vehicle and its contents are secure. Similarly, your computer, tablet, phone and other mobile devices are vehicles on the information super highway and like our car or truck, we should be in the habit of locking these devices. Just as we value the private contents of our vehicle, we should place equal value on the contents and security of our organization's computer systems and data.

Data breaches are a critical tool in keeping our network secure. In creating passwords that are effective against internal or external cyberattacks, password complexity and length must be understood. The longer and more complex the password, the harder it is to "crack". The password policy for the Arkansas Department of Health is as follows.

- Password length is 8 - 12 characters.
- No PROPER NOUNS or SPACES allowed.
- Only upper and lower case letters, numbers, and these symbols are allowed: ~ ! @ $ ^ * ( ) _ - = [] \ {} |
- These symbols are NOT allowed: % # ` & + ; : ' " , . < > / ?
- Passwords cannot contain your User Id
- Cannot reuse any of your last twenty-four (24) passwords.
- Passwords must contain at least ONE (1) NUMBER.

- BOTH UPPER and LOWER CASE letters are required.
- Passwords EXPIRE exactly ninety (90) days after they are changed. A password should be changed immediately if a user suspects that their password has been compromised.
- Users must make a good faith effort to select strong passwords, rather than weak passwords that may easily be guessed. Logical names and words, even in combination with a leading or trailing number, are weak passwords. Names spelled backwards, names of celebrities, well-known landmarks, popular culture icons, family names, etc., should be avoided.
- Sharing passwords is strictly forbidden and can result in disciplinary action, up to and including termination. This includes sharing your password with a Supervisor or co-worker.
- Written recording of password credentials is discouraged. However, if recorded, the password should not be stored in close proximity to the user's computer and should be in a secure location. When stored, the password should not be identified as such and should not include the username with the password.
- Never record a password on-line, or include a password in an email message.

It may seem like an undue task to remember long or complex passwords, but they help secure our network and therefore secure our ability to efficiently serve the public and protect their vital information.

ADH IT and the ADH Help Desk will NEVER ask you for your password. This is critical to remember, especially if you receive an Email requesting you to "click" on a link and supply your username and password to update an account or service. These types of emails are ALWAYS a scam and are designed to infect your machine with viruses or malicious software, compromising the network and exposing valuable data.

In accordance with the Arkansas Department of Health's mandatory security protocols, another security measure you should follow is to lock or power off your computer anytime you step away from it, even for a short length of time. To that end, ADH IT has set your computer to lock the screen automatically after ten (10) minutes of inactivity.

Phishing Awareness

In the Password Security section above, we learned about a specific type of scam involving receipt of a malicious email prompting you to enter in your username and password to update an account or service. We also learned that these types of emails are always a scam. These types of attacks are called "Phishing" schemes. They are so named because they try to "bait and hook" the user into providing information about themselves or the organization.

Email is an essential part of our everyday communications. It is also one of the most common methods that cybercriminals use to attempt to gain access to sensitive information. More than 90% of data breaches start with a phishing attack. Phishing uses fraudulent email messages designed to impersonate a legitimate person or organization and trick the recipient into downloading harmful

attachments or to divulge sensitive information, such as passwords, bank account numbers, and Social Security numbers.

Phishing scams typically attempt to take advantage of you by delivering file attachments that can infect your computer, enticing you to click on links to websites that infect your computer with harmful software, or by tricking you into sharing your username and password so hackers can gain access to your network or other sites.

You can identify a phishing scam by looking for email messages that: 1) creates a sense of urgency; 2) invoke strong emotions with offers that seem too good to be true; or, 3) make claims of repercussions if you do not respond. The message requests sensitive data or contains links that do not appear to match legitimate resources for the organization that is contacting you. It is important to remember that any legitimate company or organization will never ask for passwords, social security numbers or other sensitive data via email. Some helpful tips to remember to easily identify phishing schemes are as follows:

- **Don't click on attachments -** Attachments that contain viruses and malware are a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. Don't open any email attachments you weren't expecting or if you don't know who they are from.

- **Review the Email signature -** Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details. It is always best practice to include an email signature on your email message and replies. If you need help constructing an email signature, please contact the ADH Help Desk at 501-280-4357.

- **Check for spelling mistakes -** Most organizations are pretty serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious.

- **Look for Authorized banners** – All official ADH IT communications will include a banner at the top of the message (see below) letting you know that it is not a scam and that it is an authorized ADH IT message.

Vishing Awareness

Now that we have covered the basics of "Phishing" and how these attacks are perpetrated, we should also cover "Vishing" or "Voice Phishing." Vishing employs the same tactics as Phishing. However, the primary difference between the two is that Vishing attacks are carried out using voice communication instead of email communication. Vishing attacks can be carried out in several different ways. In many cases, hackers or scammers use cellular telephones, voice mail, landlines or VoIP (voice over IP) to make contact with their targets with either a live person or a pre-recorded message. Vishing can be a bit more difficult to identify because there is less to visually inspect, or the Caller ID is being manipulated to falsely identify the caller through a process called "spoofing." In many cases, the scammer will attempt to establish a sense of authority to gain your trust or push a sense of urgency and/or repercussions to confuse you, in hopes of getting you to comply with their requests. In targeted attacks, these requests usually involve the attackers posing as a "Help Desk" and attempt to convince you to download and execute remote desktop software from the internet to allow them to create a remote connection to your computer under the pretense of "fixing" problems or "removing viruses." If successful, the attackers would then have full access to your computer and the ability to download malicious software to further attack you, as well as the network. Below are some tips to help you protect yourself from Vishing attacks.

- **Educate yourself** – Knowledge is the key to defending yourself from Vishing. The more you understand it, the better off you'll be, so read up on vishing incidents. As this crime becomes more sophisticated, you will want to stay up to date.

- **Don't trust caller ID –** Caller ID can be tampered with (Spoofing) and offers a false sense of security. Politely challenge the caller; ask them to verify who they say they are. Check with your area supervisor or section chief to review or establish acceptable practices to verify your caller's identity when you receive a questionable call.

- **Challenge, Verify, Confirm -** If you receive a phone call from a person or a recording requesting personal information, hang up. If the call purports to be coming from a trusted organization, call that entity directly to confirm their request.

SMISHING Awareness

Phishing, Vishing, SMiShing OH MY! The terms keep coming because the methods of attack keep changing and evolving. SMiShing is another form of phishing that uses your smartphone's (SMS) or text messaging system, employing the same tactics as email phishing. However, this attack vector is increasingly dangerous because text messaging is so personal. We are more likely to respond to and trust a text message, even if it is from a random number, than we are to open a suspicious looking email.

"Social engineers" make a profession out of knowing how people work and operate, so they clearly and intentionally craft attacks that play on a person's biggest psychological fears and wants. They are also

aware of the fact that organizations attempt to minimize fraud and its subsequent impact through training such as this. Being so, social engineers will avoid texting ambiguous messages that do not include specific locations, organizations, websites or names. SMiShing messages are best handled by deleting them. Even texting a seemingly harmless "sorry, you have the wrong number," is an opportunity for the social engineer to respond back, open dialogue and begin to try and force the authenticity or necessity of the communication. Most SMiShing attacks are perpetrated by a real person waiting on the other end and not an automated process "bot" or artificial intelligence. Some SMiShers send texts with links that, if clicked, will install keyloggers or lead to malicious websites designed to steal personal data, while others trick targets into calling numbers that rack up outrageous charges to their phone bills.

Listed below are the best practices involved in protecting yourself from SMiShing attacks.

- Avoid clicking links within text messages, especially if they are sent from someone you don't know.
- Don't respond to text messages requesting personal information.

Laser Phishing

This form of phishing attack has earned "dishonorable mention", being that it highlights just how advanced phishing attacks have become. It gives us a glimpse into what we can expect in the near future as cyber-crime evolves. "Laser Phishing" is the automated version of email phishing. Cyber-Criminals are now using A.I. (Artificial Intelligence) to collect your information by scanning your social media profiles and posing as someone with whom you recently interacted. What makes an A.I. based attack different from a "bot" driven email attack is that the A.I. used to Laser Phish will communicate back and forth with you while posing to be a real person. The A.I. has gathered enough information to make itself seem authentic. By the time you receive an email with a malicious link, you may very well be expecting it and not think twice about clicking it. Cybersecurity researchers state that currently, awareness is about the only widespread method of combating Laser Phishing. However, it is worth mentioning because this attack vector is most often used for "whaling" or phishing for information to compromise top level administrative or organizational accounts and data.

"I Think I Have a Virus……."

If you think your workstation or device may have been infected with a virus or malware (malicious software), please make note of the behavior that lead you to that conclusion. Power off the computer and unplug the network cable. Immediately contact the ADH Help Desk at 501-280-4357 to report the issue. Next, notify your Supervisor so he or she can coordinate access to alternate resources, such as another computer or laptop. Please leave the infected device turned off until an ADH IT Technician can address and resolve the issue with the infected computer. It is important to understand that an infected

computer that remains on the network poses a risk to ALL computers connected to the network. Some of the behaviors you may experience if your computer is infected with a virus or malware are as follows:

- Pop-Up Ads
- Reduced performance or the computer running "slower than normal."
- You receive responses to emails you did not send.
- Essential tools and programs stop working
- Being locked out of your account frequently
- Mysterious behavior on your screen
- Missing items from your desktop or a blank desktop altogether
- Sudden inability to access files or folders

"What else can I do?"

Besides following the best practices discussed so far in this training module, you can become familiar with some of the safeguards in place to help minimize exposure to viruses and malware. The official ADH-sanctioned anti-virus program currently used to detect the presence of malicious software or viruses on your device is called "**CylanceProtect**." Cylance should be active on every computer in every office and in every ADH location statewide. Cylance, when running properly, can be found in the bottom right corner of the screen next to the time and date. The icon to look for will resemble a green shield with a "heartbeat" symbol. If you hover your mouse over the icon without clicking, it will display the words CylancePROTECT. You can also right-click on the Cylance icon and choose "About" to check the status of the program. If your program indicates it is not active, please contact the ADH Help Desk at 1-800-441-9232.

Social Engineering

What is **Social Engineering**? In essence, this is "people hacking". This section will focus on the often non-electronic based methods of gaining access to secure areas, buildings or computer networks. "Social engineering" is all about information gathering, person-to-person. As employees of the Arkansas Department of Health, you may have a name badge that authorizes you to be in specific designated areas. You may also have access to specific databases that others may not have. Because the attacker may be after valuable data or even physical access to the building, you become the target of these attacks.

Social Engineering Techniques
✓ Dumpster diving
✓ Shoulder surfing
✓ Tailgating/piggybacking
✓ Phishing
✓ Pretexting
✓ Intimidation
✓ Bribery

The "phishing scams" discussed in the previous section are just one form of social engineering, as well as being the most common. Another form of social engineering we need to be aware of in our work environment is "pretexting." **Pretexting** is the act of creating and using an invented scenario (the pretext) to convince a targeted victim to divulge information or perform actions they would not normally do under ordinary circumstances. In most cases, this is accomplished with an

elaborate lie. It most often involves some prior research or setup and the use of this information for impersonation (e.g., date of birth, Social Security number, last day worked) to establish legitimacy in the mind of the target.

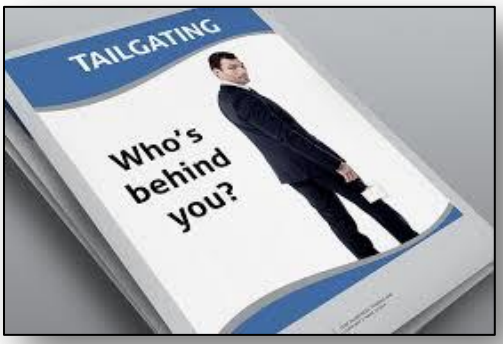
This technique can be used to fool employees into disclosing personnel information, to obtain telephone records, utility records, financial records or other information directly from department staff. The information is then used to establish even greater legitimacy under tougher questioning by a manager or administrator, e.g., to make account changes, get specific balances, etc.

Pretexting can also be used to impersonate co-workers, police, bank, tax authorities, clergy, insurance investigators—or any other individual who could have perceived authority or right-to-know in the mind of the targeted victim. The social engineer must simply prepare answers to questions that might be asked by the victim. In some cases, all that is needed is a voice that sounds authoritative, an earnest tone, and an ability to think on one's feet to create a pretextual scenario.

A good example is illustrated in the following true scenario: In February of 2016, a hacker called the FBI Help Desk and made the following statement "*I am new and I didn't understand how to get past [the portal]."* The Help Desk agent on the phone asked if the caller had an access token to which the hacker replied no. The report states the Help Desk agent then said *"that's fine-just use one of ours."* The hacker then clicked on the access token link they were provided and had full access to the computer network. Soon after that, 20,000 FBI and 9,000 Department of Homeland Security records were released to the public. The hacker accessed employees' names and even credit card information. Using the IBM 2015 cost per record breach standard ($170 per record based on malicious activity), that's nearly $5 million dollars lost during a 2-minute phone conversation. It was probably higher, given the amount of credit card data and other unknown data that was accessed.

When less direct methods of social engineering such as "phishing "and "pretexting" do not yield desired results for the cybercriminal, they have been known to try and physically gain access to a building or facility through "**Tailgating**." The following section pertains mainly to employees working at the Markham street building located in the Central Office and will cover badged access to that location. However, some of these examples can apply to Local Health Units that do control human traffic flow to and from patient areas or areas where patient information is stored.

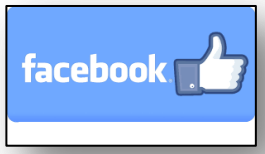
So how does Tailgating work? We have all seen that familiar face standing by the side entrance staring down at their phone. They are always so friendly, they even look up from their phone to acknowledge you, smile, and say hello or even offer to help you tote that heavy load of whatever it is you may be carrying. But who are they? Have you ever seen them use a badge? Why did they decide to go into the building behind you after you entered? This scenario is "**Tailgating**." We must acknowledge the fact that this particular lack of security awareness places the physical safety of our co-workers at risk. At the Markham street campus, no matter the situation,



anyone trying to gain entrance to an area that requires a badge MUST go to the front desk and check in with security. Users who refuse to enter via the front entrance should be reported to ADH security.

In accordance with the ADH Security Card Access policy, The Department of Health requires every employee to obtain and wear an Identification Card (ID) while on duty so that it is always visible, facing front. Extra help, part-time, and interns also must obtain and wear an ID Card. This card contains information regarding the employee's name, title and expiration date of badge, along with an identifying picture. New employees are required to obtain an ID Card within 10 working days of the start date of their employment. Employees on the Markham Street, Freeway building and Public Health Lab campuses are also required to have an additional Security Door Access Card that gives them access to specific areas within their respective buildings. ID Cards must be renewed every three years for employees and every one (1) year for non-employees such as contractors or consultants. Upon card expiration, termination, resignation, or retirement, all employees and non-employees must return their ID Card and Security Door Access Card, if applicable, to his/her immediate supervisor or primary agency contact.

Wearing your ID Badge at work is mandatory. Wearing it to lunch or after work is certainly not. Social engineers can identify routine hot spots for lunch breaks and after work rendezvous to capture glimpses of your badge and match names, faces and organizations to your social media accounts. They then mimic you online to locate a network of coworkers and other contacts. The potential threat of hackers using your social media accounts to breach the Department of Health's network is a very real possibility, if not taken care of properly. One may ask, "What does my personal social media account have to do with the ADH network?" The answer is quite simple; employees often access their personal social media accounts at work. Reviewing ADH's Social Media Policy (COM-38) will clarify there are legitimate reasons for designated users to make use of social media outlets to engage and inform the public.

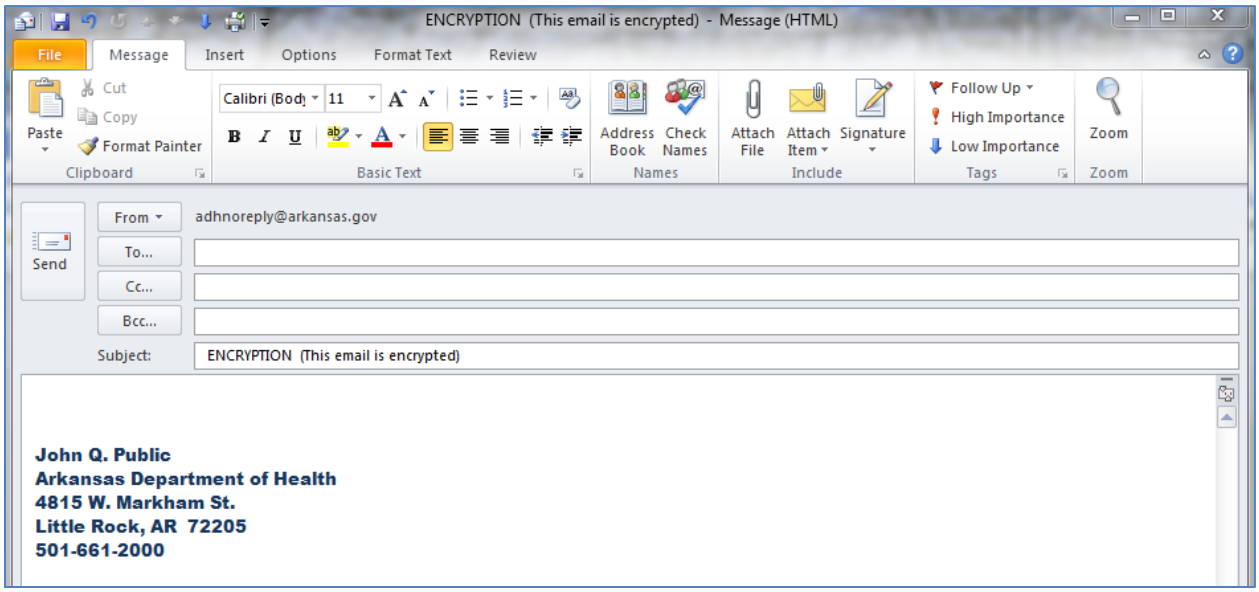


Although there are legitimate reasons to access social media accounts such as Facebook at work to complete the duties of one's position, supervisors are charged with monitoring the use of social media accounts and enforcing the ADH Social Media policy. If such use is deemed inappropriate, disciplinary action can occur. Minimizing or ceasing the use of personal social media accounts in the workplace contributes to minimizing the risk of compromising all Arkansas Department of Health assets.

The prevalence of social media and its allure is undeniable and extremely attractive to would-be and actual cybercriminals. Using methods such as hijacking accounts or creating fake social media accounts, cybercriminals capitalize on the addictive nature of acquiring friends on Facebook or professional contacts on LinkedIn. They may attempt to lure you into clicking on the baited friend request, an interesting news story or game request, allowing your computer or device to become compromised. When it comes to thwarting the never-ending efforts of cybercriminals attempting to hack into networks and steal identities or information, one should always remember this simple rule. "**Stop. Think. Connect**."

Secure Email Messaging

When situations arise that require the ability to send an email in a secure manner, ADH provides a simple and easy way to do so. In most cases, if you are sending an email with sensitive information or PHI to someone outside of ADH, you should send it using the secure delivery method. ADH users have the ability to send Secure Email by using the follow procedure:



1. Create a new email message in Microsoft Outlook.

2. In the **Subject** line: Enter a space, the word ENCRYPTION (all caps or lower case, either is correct), and another space.

3. It is **CRUCIAL** that you enter a space both before and after the word Encryption, as this is what causes the email to become secure.

4. Once you have entered **(space) ENCRYPTION (space),** you may then enter any other information in the ***Subject*** line that you would like to include. The key is in making sure there is a space both before and after the word Encryption.

Email sent from an ADH authorized email address in this fashion will be sent in a secure manner. Any other email entity that maintains exchange server tokens, (UAMS, Gmail, Hotmail, etc.) will allow the received email to be read without the need for a token to unlock it, or for any other actions. However, email received by an entity that does not maintain exchange server tokens will advise the user they must go to a website where they will be required to validate their identity before being able to read the secure email.

Remember that although your email may have been sent as secure when it left your mailbox, once it leaves your system and is received by other individuals, you are no longer able to maintain its' security. Emails inadvertently sent to the wrong address, although secure, could allow PHI to fall into the wrong hands. Keep in mind that emails can be copied, forwarded, etc., with no guarantee that the individual doing so will continue to send the information in a secure

manner. It is always best to ensure that anytime you send information outside the agency in a secure fashion, you know the individual and trust them to guard the information carefully.

Sending secure email to a distribution list should be avoided. There is no way to know for sure if all the users on the distribution list are the correct people to receive protected information. It is the sender's responsibility under HIPAA to securely deliver the message to the designated recipient at the address provided by the recipient…. Not to a distribution list.

Mobile Devices and Removable Storage

ADH devices such as laptops, tablets and cell phones can be found in nearly every corner of the state. State issued devices have the ability (if authorized) to connect to the ADH network remotely either through a Virtual Private Network (VPN) connection or RDWeb. They also have the ability to send and receive official agency email and communications. Devices such as USB (removable storage or thumb drive) drives used for official ADH use must be encrypted and must be closely tracked at all times. All files on the encrypted drive should be scanned for viruses **before** connecting them to any ADH system. ADH policy states that ADH work related data must be stored only on ADH issued media. You cannot load, use or store any ADH work related information, files or date on a personal non-ADH device. If you do not have an encrypted removable storage device or thumb drive, one can be checked out from the ADH IT department. All media not issued by ADH can only be used after being approved by the ADH Chief Information Officer and loaded with encryption software. All protected health information (PHI) and all official ADH work related data (including pictures) must be on an ADH IT issued encrypted drive. If large files are involved, an SFTP (secure file transfer protocol) connection may be used to deliver information in a secure fashion. Contact ADH IT for more information about using an SFTP connection. All data transferred to a portable storage media device must be classified pursuant to the State of Arkansas DIS Data and System Security Classification Standards. This standard applies Criticality and Sensitivity levels to data. A summary of these levels is listed in the ADH Removable and Portable Storage Media policy. All data placed on a removable and/or portable storage media must be encrypted with ADH approved encryption technology and the use of a complex password.

All removable and/or portable storage media must be secured in locked facilities when not in use. Employees who have been issued removable and portable storage media are responsible for the security of the device and the data on the device. Encryption software must not be removed by the user. Missing or stolen storage media (i.e. laptops, tablets, cell phones, USB drives) must be reported immediately on an Occurrence Report (AS-8) and a copy should be sent to the ADH IT CIO. All removable and portable storage media that is no longer useable or no longer functional must be returned to the ADH CIO for destruction.

All agency issued cell phones must have the encryption options turned on, if available. If the device does not offer an encryption option, then password protection or key lock features must be turned on.

Security Mentor Program

In addition to ADH's annual Cybersecurity Awareness course, all state agencies are now participating in a mandatory, web-based, interactive Cybersecurity training program from ***Security Mentor***. Every other month, *Security Mentor* releases a training module covering a specific topic. The modules are designed to help you understand cyber threats and how to protect yourself and your organization from them. Availability of new modules will be sent to your ADH email address, as noted below:

Security Mentor, Inc. lesson-notice@securitymentor.com

Lessons take an average of 15 minutes or less to complete. In addition to being informative, the lessons can often be entertaining due to the interactive learning platform. Also, please contribute to the surveys at the end of the lesson modules to assist Security Mentor in being able to provide improved content based on user feedback.

Remember – the best security to protect against cybercriminals is you. "**Stop. Think. Connect**."