ECS
Serving Your IT Needs

Mobile Device Protection

“The best defense is a good offense”. Rather than reacting to attacks once they’ve occurred, a wise strategy is to prepare proactive measures, so that if the time comes, you can completely bypass the attack, or lessen the blow of it.

No Credit Card Numbers

Many times, it seems convenient to store credit card numbers on your phone so you have them at your fingertips and you don’t necessarily have to rely on your memory. But just as it is easy for you to access these numbers, it is easy for someone who means harm to access them.

If for some reason it is absolutely necessary for you to store this information on your phone, it is important for you to take extreme measures to make sure the data is safeguarded, such as tokenization and/or encryption.

Place Lock on Phone

Enabling a lock on your phone when not in use, and a pin or password to unlock the phone could help prevent unauthorized use of the phone. Just as we talked about in a previous module, if you set a password on your phone, it is important to create a strong password.

Keep these tips in mind when creating your password:

- Use a unique password for each of your accounts. Do not use one password for all of them.
- Ensure your password consists of letters, numbers, and symbols. This would make it harder for others to figure out.

- Avoid using common words or consecutive characters to make up your password (e.g., Do not use “password” as your password. Do not use a password such as Office111).

Don’t Save Passwords

When it comes to passwords, the ideal situation would be to remember them so there is no trail of what they are, which could make it easy for an unauthorized user to utilize them. But the fact is, most people have unique passwords for each account they have. Because of this, it may be necessary to use a back-up method in case they are forgotten. If this is the case, write them down and securely store them. Do not save them on your phone.

- Write them down and treat them as you would any other important documents by locking them in a safe or drawer that requires a key.
- Invest in a password manager service.

No Personalized Contacts Listed

You’ve created a lock on your phone and regularly lock it when it’s not in use. You quickly step away from your desk with your phone on it, and forget to lock it. Someone who doesn’t have permission to touch your phone decides to go through your contact list. John sees the name Bob Jones with “ABC Company Manager” in parentheses. John writes down Bob’s name and number and decides to use it to solicit Bob’s business.

This is one scenario of what can happen when your phone includes a personalized contact list. In this example, the result, while uncomfortable, is not an extreme situation. Just think what could have happened!

Practical Illustration

Delores and Earl have recently been given cell phones by their company to be able to conduct business while they are away from the office. Their manager encourages them to lock their phones each time they are not in use and make sure they memorize the password to unlock it. Delores tells Earl that she's happy they have the phones because she can save her customers' credit card information on it so she doesn't always have to refer to her paper file when she needs to conduct a transaction for them. Earl states that it is best not to do that because if her phone gets hacked, the customers' financial data may be compromised.

Review Questions (Please watch video or listen to audio file for right answers)

1. Credit card numbers:
    a. Should only be stored in your phone if you have less than three credit cards
    b. Should only be stored in your phone if you have less than two credit cards
    c. Should always be stored in your phone
    d. Should not be stored in your phone, if possible

2. What is a way to safeguard credit card information that you must store on your phone?
    a. Encryption
    b. Tokenization
    c. A and B
    d. None of the above

ECS
Serving Your IT Needs

3. When setting up a lock on your phone that can be opened with a password:
    a. Use a password that is the same as all of your other passwords
    b. Use a password that is different from all of your other passwords.
    c. Use a password that has no more than five characters
    d. Use a password that has no more than three characters

4. To create a strong password, it should have:
    a. Letters and numbers
    b. Numbers and symbols
    c. Letters, numbers, and symbols
    d. Letters and symbols

5. What should be your back-up method if you cannot remember your password?
    a. Write down and place in a secure location
    b. Save it on your phone
    c. Write it down and leave it with a person you trust
    d. Any of the above

6. The “Don’t Save Passwords” lesson states that passwords should be secured where?
    a. In a co-worker’s files
    b. On the main screen of your phone
    c. In a closet
    d. In a safe

7. What is the name of the person in the contact list?
    a. Bill Johnson
    b. John Taylor
    c. Jim Smith
    d. Bob Jones

8. What was the job title of the person in the contact list?
    a. Quality representative
    b. Manager
    c. Account manager
    d. Client relations representative

9. What should you NOT save on your phone?
    a. Customers' credit card information
    b. Passwords for social media accounts
    c. Your boss' birthday
    d. The address to a client's office

10. How can you protect your phone privacy?
    a. Recharge phone every three hours
    b. Only use phone after 2:00 p.m.
    c. Save passwords on phone
    d. Lock phone when not in use