CYBER SECURITY AWARENESS MONTH

WEEK 4: Our Continuously Connected Lives: What's Your 'App'-titude?

Chipped Credit Cards:

Why chip cards are safer than magnetic stripes on debit/credit cards

Since January 2016, a large number of retail companies that accept credit cards have made the switch to chip credit cards. The reason is because chipped credit cards are more secure. Chip cards are technically known as EMV cards, named for the 3 major credit companies that backed the development of the technology: Europay, MasterCard, and Visa.

> "...fraud has been a problem that has cost credit card companies billions annually for years."

To understand how a chip card is more secure, we must first understand how credit card payments work with the magnetic stripe. On a credit card's magnetic stripe, account information such as credit card number and expiration date is encoded with no real security measures built in. Credit card machines simply read the data and record the transaction amount. An unscrupulous merchant, employee, or thief could "skim" or record and save the credit card owner's magnetic stripe data for fraudulent use later. Usually the credit card data is bought and sold online for use in online credit fraud. Another more brazen use is to magnetically load dummy credit cards with the stolen data to be used in "brick and mortar" retail stores. However it's carried out, fraud has been a problem that has cost credit card companies billions annually for years.[1]

The chip card surpasses the magnetic stripe technology in its sophistication. No longer is user data blindly copied from the credit card; with a chip card, each transaction is encoded with a unique ID and the transaction data is encrypted by the card itself. The chip inside the chip card is a mini computer. It can store information as well as encrypt transaction details that are passed through the chip. By both encrypting the data and issuing a unique transaction ID, it is difficult for anyone to issue a fraudulent transaction ID or recreate the encrypted transaction information. As with any technology, it is not absolutely free from being exploited by the most determined hacker, but it does greatly increase the complexity and difficulty of stealing and using credit card data from the Point of Sale.

The chip credit card is just another example of where encryption helps ensure a reliable and trustworthy exchange of sensitive information in an otherwise unsecure world.

[1] Sidel, R. "Cost of Credit-Card Fraud is Set to Shift." The Wall Street Journal, 29 Sep. 2015, http://www.wsj.com/articles/card-liability-is-set-to-shift-1443567562. Accessed 21 Oct. 2017.

For more information on EMV credit cards, please peruse the following resources:

Kossman, S. "8 FAQs about EMV credit cards." CreditCards.com, 29 Sep. 2016, http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php. Accessed 21 Oct. 2017.

Pagliery, J. "New Security Flaw in Credit Card Chip System Revealed." CNN Money, 5 Aug. 2016, http://money.cnn.com/2016/08/03/technology/credit-card-chips-flaw/. Accessed 21 Oct. 2017.

Workman, K. "Confused by Chip Cards? Get in Line." The New York Times, 5 Aug. 2016, http://www.nytimes.com/2016/08/06/business/chip-credit-cards-for-dummies.html?_r=0/ Accessed 21 Oct. 2017.

Suggested Classroom Activity: Public Key Encryption

Public key encryption is a cryptographic system that uses two keys - a public key known to everyone and a private or secret key known only to the recipient of the message. For example, when John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it. This is the method used by chipped credit card readers to encrypt transaction details. The credit card contains the private key and the card reader uses its public key algorithm to combine with the private key and encrypt all transaction data. Read through these online resources for more information on public key encryption:

Word to the Wise Blog. "Cryptography with Alice and Bob." Word to the Wise, 17 Sep. 2014, https://wordtothewise.com/2014/09/cryptography-alice-bob/. Accessed 21 Oct. 2017.

Wikipedia. "Alice and Bob." Wikipedia, https://en.wikipedia.org/wiki/Alice_and_Bob. Accessed 21 Oct. 2017.

As you can see with the above references, public key encryption is typically referred to with names such as Alice and Bob not John and Jane. Those names act as alphabetical placeholders for data. Discuss with students how public key encryption works and see if they can create a method of encrypting messages using this method.