Did You Know?

October is National Security Awareness Month.

There have been a total of 579 data breaches in 2014, exposing nearly 77 million records. 41 of the breaches have occurred in education companies, equating to 1.5 million records.

Sources:
Crn.com
Msisac.cisecurity.org

Security Terms

Tokenization:
The process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security.

Need to report an incident?
Send an email to the Security Response Team SRT@careered.com

Welcome to Career Education Corporation’s information security quarterly newsletter. This newsletter aims to reinforce good information security habits, teach best practices, cover emerging issues and report on interesting information security news.

Does ‘Apple Pay’ Keep the Hacker Away?

During the most recent Apple keynote address, a "new, easy, secure and private" method for mobile payments was unveiled, called Apple Pay. Although the technology behind Apple Pay has been in use for some time, security analysts are reviewing Apple’s take on the digital wallet to determine if it is in fact a move in the right direction.

For starters, Apple won’t store any credit card numbers or transaction information on its servers or in their devices. Instead, a technology called "tokenization" will be used to identify a user and device for payments.

When a person adds a credit card to their iPhone, instead of storing the user’s actual credit card number, another account number is generated to identify the user and device (the token). This device-only account number is stored in an encrypted chip in the iPhone 6, 6 Plus and Apple Watch called the “secure element”.

In the event the token is captured by a would-be hacker, it will be useless to them without a variety of other information about the user. This could potentially increase the risk of Apple device theft, but in the event of theft, or loss, Apple has updated its Find My iPhone feature to place devices in lost mode to prevent any access to the device, in addition to the ability to remotely wipe the device.

Apple Pay utilizes a secondary method for validating the transaction is from a valid user. Either the iPhone’s Touch ID fingerprint reader can be used, or a secure PIN code.

As with any new technology, Apple Pay will need to be tested thoroughly to see if it is all it promises to be.

CIS Cyber Security Pledge

October is National Cyber Security Awareness Month. In recognition of the important role each of us plays in securing cyberspace, review the following pledge.

I pledge to:

- Take personal responsibility for security and use good security practices
- Pause and consider the risk before I connect to the Internet
- Lock my computer whenever I leave my work area
- Treat my mobile device like the powerful computer it is, and protect it – both physically as well as by activating security features such as passwords and anti-lock, anti-virus software, and remote wiping
- Use strong passwords, and create a separate one for each account
- Never share my password with anyone
- Follow my organization’s policy and promptly report all security incidents or concerns to my organization’s security office or contact
- Safeguard sensitive data from any inappropriate disclosure
- Not post personal, sensitive, or non-public information on social media
- Not participate in any cyber bullying activities
- Raise awareness of good security practices among my family, friends, colleagues and community.
Want to provide feedback or suggestions on this newsletter? Send an email to the Information Risk Management team: InformationRiskManagement@careered.com

**Tips & Tools**

This section is used to provide information about security tips or tools that you can utilize on your personal computers. Please note, CEC does not support these tools (please don’t contact the Service Desk for assistance).

The SANS Institute has a “Security Awareness Tip of the Day” on their site. It offers some good practical advice for keeping you and your data safe in the online world.

[http://www.sans.org/tip_of_the_day.php](http://www.sans.org/tip_of_the_day.php)