



**From the Office of Information Management Technology**

Below are highlights of several of these new advancements and how they may affect us.

A Bitcoin is a digital currency stored in a downloadable wallet on a user's personal computer or with an online wallet service provider. Each wallet has a unique identifier that allows users to transfer bitcoins to other users' wallets. Bitcoin is a decentralized, peer-to-peer payment

<sup>1</sup> <http://www.businessinsider.com/russia-claims-china-bugged-tea-kettles-2013-10#ixzz2nM6vxMX8>

system, currently with no regulatory authority. It is gaining popularity, with mainstream businesses adopting it as an alternative form of payment or investment.

While the long-term use of Bitcoin is uncertain, for at least the near term in 2014, the increasing adoption and publicity will continue to draw the interest of cyber criminals who target Bitcoin users' wallets for theft, or compromise systems to generate bitcoins via malware infection.

---

## Mobile Transaction Risks

Every new smart phone, tablet or other mobile device provides an opportunity for a potential cyber attack. New features such as Near Field Communications (NFC), as well as AirDrop and Passbook for Apple, will continue to expand in 2014, increasing the opportunities for cyber criminals to exploit weaknesses. NFC and AirDrop allow for similarly configured smartphones to communicate with each other by simply touching another smart phone, or being in proximity to another smartphone. This technology is being used for credit card purchases, boarding passes, and file sharing, and will most likely be incorporated into other uses in 2014.

Risks of these technologies could include eavesdropping (through which the cyber criminal can intercept data transmission such as credit card numbers) and transferring viruses or other malware from one NFC/AirDrop-enabled device to another.

---

## Summary

Before adopting any of the myriad new technologies that are rapidly being deployed, it's important to understand the implications and risks. While interconnectivity can yield many benefits, the risk could outweigh the benefit if the devices, systems and technologies are not properly secured.

---

## For More Information

### Georgia Tech: Emerging Cyber Threats Report

<http://www.gtsecuritysummit.com/2014Report.pdf>

### Sophos: Security Threat Report 2014

<http://www.sophos.com/en-us/threat-center/security-threat-report.aspx>

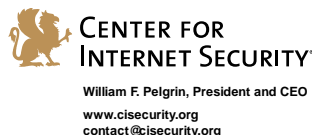
### WebSense: 2014 Security Predictions

<http://www.websense.com/2014predictions?cmpid=prnr11.14.13>

### Symantec: 2014 Predications

<http://www.symantec.com/connect/blogs/2014-predictions-symantec-0>

Provided By:



*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.*

*Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.*