FINANCIAL INSTITUTIONS AND THEIR AUTHENTICATION

In a perfect world, the more data points your financial institution has, the stronger the identity and privacy protection it can provide. By definition, the Internet of Things should allow an institution more data points for purchase and identity verification, which will lead to greater protection for you.

A recent example is the growing use of new debit and credit cards equipped with a computer chip, designed to improve data security and reduce the risk of identity theft. The chip syncs up with the point-of-sale device at the store, verifying the authenticity of the card.

In the future, biometrics should also assist in the authentication process in digital financial transactions, with wearable technology increasing this potential. Finally, the GPS capabilities on virtually all mobile devices can help to validate a specific person's whereabouts as part of the authentication process.

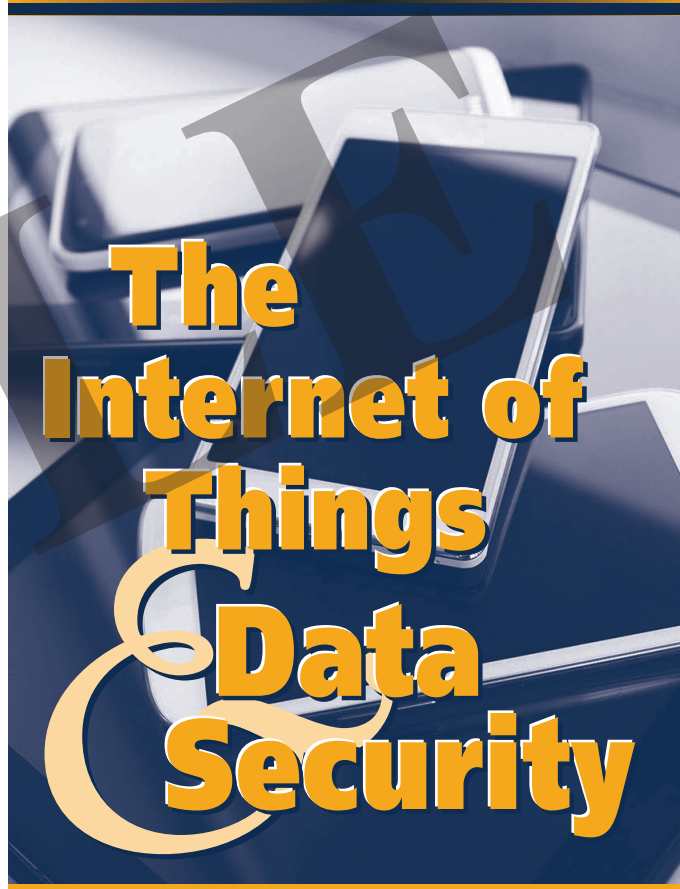
* Your Security Takeaway:

- ☑ Financial institutions are developing complex digital payment systems, like chip cards, to make transactions safer.
- ☑ Financial institutions are investing heavily in internal computer security and training to safeguard your personal financial information.
- ☑ Regulators and industry workgroups are constantly developing new measures and means to guarantee the safety and security of online financial transactions.

While the Internet of Things phenomenon is poised to transform our lives—allowing us to remotely access, monitor and control our home devices via the Internet—it will also make securing all our devices a most important priority. Your financial institution is committed to meeting this priority, and to helping you understand the risks, learn how to mitigate them, and understand why it is so important to remain vigilant when using the unprecedented convenience of online banking and the Internet of Things.

RESOURCES

- **Stopthinkconnect.org**
- Federal Trade Commission: **http://www.ftc.gov**
- U.S. Treasury Department: **http://www.treasury.gov**
- Identity Theft Resource Center: **www.idtheftcenter.org**



The Internet of Things & Data Security

Our increasingly internet-connected future will mean safer transactions…and added security responsibilities for all of us.

FROM DESKTOPS TO SMARTWATCHES

Just a few years ago, Americans conducted online financial transactions mostly through desktop-based personal computers. Now, connectivity comes in many forms. Today's household, for example, might include one or more of the following: smartphone, tablet, laptop computer, desktop computer and smartwatch, any one of which can be used to connect to an online account—and *with each other in some cases*. Experts call this interconnectivity—the Internet of Things, a term you will likely hear more and more as the technology develops.

With increasing numbers of devices having embedded operating systems comes a wealth of new opportunities for the end user. Whether using your laptop to access your accounts, a Smartwatch to collect your health data, or your Smartphone to receive firmware updates, what we see as added value, criminals view as opportunities.

INTEGRATED SECURITY

One of the best ways to protect yourself is by taking an *Integrated Approach* to security. This simply means being aware of where your risks might lie, then addressing each of these risks.

1. Make an inventory of all your Internet connected devices—phone, tablet, computer, Smartwatch, etc.
2. Evaluate how each device is protected from hackers and malware.
3. Assess your risk. Can a hacker gain access to any or all of your devices?
4. Purchase and install the appropriate software protections for each device.

Of key importance: Pay attention to the Wi-Fi router in your home—it is the main way devices connect to the Internet. Use a strong password, name the device in a way that won't let people know it's your house, and keep the router software up to date.

✱ Your Security Takeaway:

- ☑ Treat your mobile phone, tablets and other devices like your computer. Use strong passwords and security settings.
- ☑ Install and regularly update security software and firewalls on each of your internet connected devices.
- ☑ Build strong protections around your Wi-Fi router, the main port through which your transactions are conducted.

WIRELESS NETWORKS AND HOTSPOTS

Public Wi-Fi and hotspots are very convenient, but not very secure. To be safe, avoid performing financial transactions on a public network. If you need to access your account, try disabling the Wi-Fi and switching to your mobile network. Keep in mind that the decidedly low-tech problem of a *stranger looking over your shoulder* is still one of the biggest threats to your online security when you are in public.

✱ Your Security Takeaway:

- ☑ When conducting financial transactions in public, disable Wi-Fi and switch to your mobile network.
- ☑ Be wary of strangers watching your transactions.

Things by the Numbers

Where is the Internet of Things today...and where is it headed? Experts have some predictions.

- **87%** of the U.S. population ages 18 and above own or have regular access to a mobile phone, according to Federal Reserve surveys.
- **30.7 billion**—The number of consumer devices that collect and store data every day. Experts believe the figure will explode in the next 5 years. By 2025, 75.4 billion connected devices will be in use by consumers.
- **A recent security report** stated that only 59% of companies are encrypting all consumer data they collect. Fewer than half of the companies could detect every breach.