MOBILE PAYMENTS AND BANKING TIP CARD

More and more frequently, consumers are using their mobile devices for online banking, payments, and shopping. We can now check our bank account balances, deposit a check using a mobile device's camera, pay bills, transfer money between friends, and make purchases directly on our mobile devices. However, since these activities require users to provide sensitive personal information such as their names, account numbers, email addresses, and passwords, it is important to weigh the perceived benefits and potential risks associated with mobile payments and banking.

DID YOU KNOW?

- More than half of adults (51 percent) bank online and 32 percent of adults bank online from their mobile device.[1]
- Young adults between the ages of 18 and 29 years old are leading the mobile banking trend, with 54 percent banking on their mobile devices.[2]
- 22 percent of all mobile phone owners have made a mobile payment, up from 15 percent in 2012.[3]
- 62 percent of non-mobile payment users cited concern about the security of the technology as the reason for not using mobile banking or mobile payments.[4]

SIMPLE TIPS

Follow these tips from the Stop.Think.Connect.™ Campaign and the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) to protect yourself when using mobile devices for online banking, payments, and shopping:

- **Use stronger authentication.** Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email or bank accounts. A stronger authentication helps verify a user has authorized access to an online account. For example, it could be a one-time PIN texted to a mobile device, providing an added layer of security beyond the password and username. Visit www.lockdownyourlogin.com for more information on stronger authentication.
- **Make strong and complex passwords.** Create a password with 8 characters or more and a combination of upper and lowercase letters, numbers, and symbols.
- **Use unique passwords.** Use different passwords for different programs, accounts, and devices. By having multiple passwords, even if attackers do get one of your

[1] Pew Research Center, "51% of U.S. Adults Bank Online", August 2013.
[2] Ibid
[3] Board of Governors of the Federal Reserve System, "Consumers and Mobile Finances", March 2015. [4] Ibid

passwords, they will not have access to all of your accounts. Do not choose options that allow your device to remember your passwords.

- **Check your account statements regularly.** Review your banking, credit card, or payment service statements regularly to ensure there are no unauthorized charges or withdrawals.
- **Know your applications.** Be sure to review and understand the details of an app before downloading and installing it. Be aware that apps may request access to your location and personal information and determine what information you want the app to be sharing or transmitting. Delete any apps that you do not use regularly to increase your security.
- **Review social media permissions.** If a payment service is linked to your social media account, your payment or purchase history could accidentally be shared with your larger network. The more you post about yourself, the easier it might be for someone to use the information you post to access your accounts, steal your identity, and more. Be sure to review and understand those privacy permissions and settings.

Stop.Think.Connect. is a national public awareness campaign aimed at empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family and your community. For more information visit www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™