Consumer Credit Counseling Service (CCCS)
Of Central Oklahoma

405-789-2227 1-800-364-2227 Spring 2013

cccsok.org

Your High Tech, James Bond Gadget Could Put You in Financial Danger

There are more than two dozen James Bond movies, and in each one, 007 uses clever gadgets, allowing him to thwart the bad guys. The first Bond film hit big screens in 1962 (*Dr. No)*, and since then, Mr. Bond and his villains have made the most of some creative and destructive devices. That was Hollywood. This is today, and some of that technology has become reality.

Take smart phones, and other wireless mobile devices for example. Some estimates say more than one billion people use them daily. (That would even impress Q, the character who supplies Bond with gadgets).

Cell phones, once used to talk, now allow you to transfer money, store sensitive financial records, save important notes and much more. Those devices are useful, but they come with risk. 007 would caution you, be careful where you leave your device! A villain, henchman, or simple thief bent on stealing your money or identity may need to do nothing more than snag your mobile device.

Banks and financial institutions have safeguards to protect your money and information. But those firewalls are not 100% fool-proof.

First, take a look at range of services:

Text, or SMS (short message service): This services allows you to get account information, like your balance. You can also receive alerts via text message.

Mobile device banking: This allows you to log onto your account using your device's web browser. You can do all your online banking with this service.

Apps: These are programs that you download and are hugely popular because they are quick and easy to use, and make navigating a small screen much easier. Increasing numbers of banks, credit unions and other financial institutions are creating apps that allow you to snap a photo of a check, then deposit it into your account.

Mobile web payments: This allows you to purchase stuff. Think, "shopping at Macy's, from the beach!"

Mobile text (SMS) payments: Allows you to make purchases via text message, hence the nickname, "text to buy." This purchase may be added to your wireless service bill, or a pre-registered credit/debit card, payment service account or digital wallet. Used for small items, like ringtones, music, etc.

Mobile point-of sale payments, aka "Proxi Payments": Tap or wave your device past

Who is CCCS?

Consumer Credit Counseling Service of Central Oklahoma has served Oklahomans since 1967.

We are a part of the United Way in several Oklahoma communities and we are all living and working in Oklahoma, just like you.

We provide free counseling services whether or not you choose to enroll in our Debt Management Plan.

Our mission statement reads:

"CCCS is a non-profit agency committed to helping people help themselves become financially strong individuals and families through counseling, debt management and education".

We honestly want what is the best for our clients—which is why we have been the trusted professionals in this area for so many years.

an electronic reader at the check-out stand and your good to go.

P2P: "Peer-to-peer" payments are informal transactions between two individuals. You just need an app, or touch two smart-phones together.

Anytime sensitive information is sent with your wireless device, your data could be vulnerable.

Bad guys can use viruses, spyware and other programs to steal your data, and/or cause harm to your mobile device.

Protect Yourself

Your bank, credit union or other financial institution has likely taken aggressive steps to ensure your transactions are safe and secure. They are very serious about protecting their customer's information. You, however, should still keep up your guard! Theft of money and personal information can have massive ripple affects that can haunt you for years.

- Handle your mobile device like you do your wallet, since your mobile device contains a lot of the same stuff (and maybe more) than your wallet!
- Think twice about loaning your device. You wouldn't let some guy on the street walk up and say, "hey, can I take a look inside your wallet?"
  - So why would you loan your I-Phone to someone you don't know and/or trust?
- Ask your provider if you have the ability to remotely delete contents on your device. This could be a handy feature if your device gets lost or stolen.
- Use strong passwords. Think like 007!
  - Strong passwords have eight characters or more, with upper and lower case letters, and numbers and symbols.
  - Change passwords often.
  - Change it immediately if you think your password is compromised. (Think about the problems that could arise if an ex-boyfriend or girlfriend, former friend, or arch nemesis, has access to all your financial information).
- Log-it-off!
- Turn off the Bluetooth.
- Never send sensitive info through email or instant messages since they probably are not secure.
- Don't use public Wi-Fi for shopping and banking. You might as well open your wallet, and leave it sitting on a table at the mall.
- Watch your accounts. Look at them daily, or at least weekly.
  - The sooner you report fraudulent activity to your bank, the more likely your bank will protect some or all losses.
  - In most instances, you must report fraudulent activity within a few days. Some may allow you to report within 60 days. Check with your bank for their exact policy.
  - Use credit and debit cards that offer protection. (Ask for the for details.)
- If you lose your mobile device, call everyone with whom you conduct wireless business, and ask for their advice.
  - This will also put them on notice that your wireless wallet is missing. They can help you disable passwords and protect your accounts.

Wireless devices have made life more convenient in so many ways, but only if you remember to protect yourself. It can be difficult living in this new age of James Bond gadgets. You, however, can avoid many of those issues by protecting yourself so your *Diamonds Are Forever!*