MOBILE SECURITY TIP CARD

Mobile devices enable Americans to get online wherever they are. Although mobile devices — from smart watches to phones and tables — can be extremely useful and convenient, there are also potential threats users may face with such technology. It's important to understand how to protect yourself when connecting on the go.

DID YOU KNOW?

- **56 percent of American adults** own a smartphone.[1]
- **More than half of mobile application (app) users** have uninstalled or decided not to install an app due to concerns about their personal information.[2]

SIMPLE TIPS

1. **Use strong passwords.** Change any default passwords on your mobile device to ones that would be difficult for someone to guess. Use different passwords for different programs and devices. Do not choose options that allow your device to remember your passwords.
2. **Keep software up to date.** Install updates for apps and your device's operating system as soon as they are available. Keeping the software on your mobile device up to date will prevent attackers from being able to take advantage of known vulnerabilities.
3. **Disable remote connectivity.** Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can connect to other devices. Disable these features when they are not in use.
4. **Be careful what you post and when.** Wait to post pictures from trips and events so that people do not know where to find you. Posting where you are also reminds others that your house is empty.
5. **Guard your mobile device.** In order to prevent theft and unauthorized access, never leave your mobile device unattended in a public place and lock your device when it is not in use.
6. **Know your apps.** 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. Delete any apps that you do not use regularly to increase your security.
7. **Know the available resources.** Use the Federal Communications Commission's Smartphone Security Checker at www.fcc.gov/smartphone-security.

[1] Pew Research Center's Internet & American Life Project, May 2013

[2] Pew Research Center's Internet & American Life Project, May 2013

RESOURCES AVAILABLE TO YOU

US-CERT.gov

US-CERT provides tips for both individuals and organizations on how to protect against cyber threats. Visit www.us-cert.gov/cas/tips for more information.

OnGuardOnline.gov

This website, run by the Federal Trade Commission (FTC), is a one-stop shop for online safety resources available to individuals of all ages.

StaySafeOnline.org

The National Cyber Security Alliance offers instruction on security updates, free anti-virus software, malware software removal and other services.

IF YOU ARE A VICTIM OF ONLINE CRIME

- Immediately notify your local authorities and file a complaint with the Internet Crime Complaint Center at www.ic3.gov.
- If you think a site has collected your personal information in a way that violates the law, report it to the FTC at www.ftc.gov/complaint.
- If someone has had inappropriate contact over the Internet with you or a colleague, report it to www.cybertipline.com and they will coordinate with the Federal Bureau of Investigation and local authorities.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and 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™

Jim Garrett CISSP, ISO27001/2 Lead Assessor, GCFA, MBA
Interim Chief Information Security Officer
University Hospital
garretig@uhnj.org
Office: 973-972-2123
Help Desk - 3-3200

UNIVERSITY HOSPITAL
Newark, New Jersey