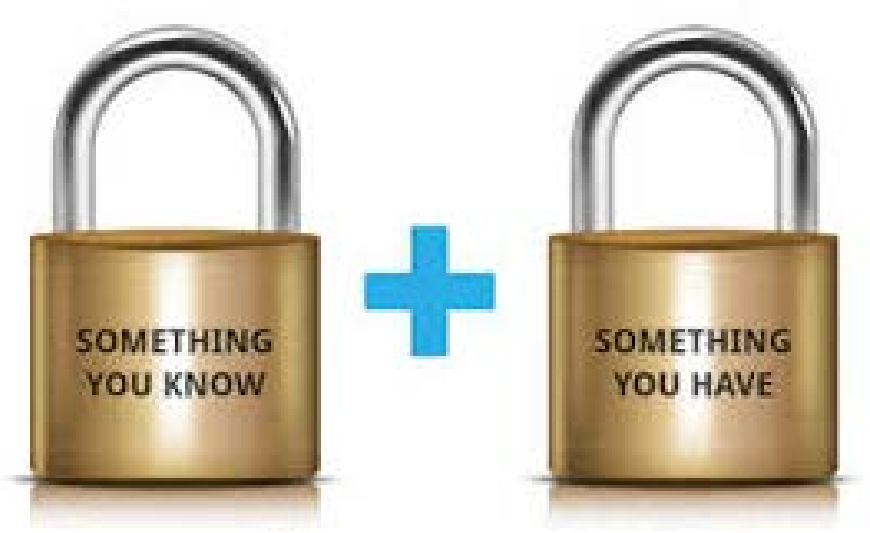

UTHSC G.U.A.R.D.

Summer 2017

IN THIS ISSUE

Two-factor Authentication: Better Security

by Chris Madeksho, Information Security Coordinator

Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. Typically, 2FA provides better security than single-factor authentication (SFA), a security process in which the user provides only one factor -- typically a password.

Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive information, and online services are increasingly introducing 2FA to prevent their users' data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain users' passwords.

The ways in which someone can be authenticated usually fall into three categories known as the factors of authentication, which include:

1. **Knowledge factors** -- something the user knows, such as a password, PIN or shared secret.
2. **Possession factors** -- something the user has, such as an ID card, security token or a smartphone.
3. **Biometrics** -- something the user **is**. These may be personal attributes mapped from physical characteristics, such as fingerprints, face and voice. It also includes behavioral biometrics, such as keystroke dynamics, gait or speech patterns.

Two-factor authentication a combination of any two of the above three ways, usually 1 and 2, as biometric authentications can be the most cost prohibited.

Two-factor authentication is one of the best steps to take to secure any account. For more information on this topic or any security issues, contact the Information Security Team at itsecurity@uthsc.edu or (901) 488-1579.

Passwords may not be enough

Get information on two-factor authentication and why it is more secure that just a password

Traveling?

Keep cyber security in mind when traveling with your mobile devices

Cyber Security Tips When Traveling this Summer

by Chris Madeksho, Information Security Coordinator

There are certainly many gadgets and devices to choose from to stay connected while travelling today. Whether it's a smartphone, laptop, notebook, tablet, all-in-one or any combination, you still need access to the Internet. Unfortunately, there are bad people out there that specialize in preying on unsuspecting travelers in unfamiliar surroundings just trying to get "connected." Whether it's getting some work done while on vacation (hopefully not), staying connected with family and friends, or just surfing the Web, hackers know you want to connect and they will do their best to get in the middle of those plans so they can access your device and/or important data, not to mention being more than willing to just steal the device itself if they can.

So with vacation season in full swing, the Information Security Team wants to offer some tips and advice to help keep your sensitive information and personal devices safe from possible threats.

- **Password protect your device** – we cannot emphasize this enough. If it has a screen lock, protect it.
- **Make sure your applications and antivirus software are up-to-date before you leave** – you don't want to rely on an unsafe connection while you're travelling to do it.
- **If possible, install a firewall** – this will provide an added layer of protection against unauthorized access.
- **Limit password attempts** – some devices have an option that will erase all data if the password is entered incorrectly 10 times. Enable this option so that if you lose the device, that is all you'll lose.
- **Gotcha tools** – you may want to look into anti-theft measures, like remote locking and/or tracking. Some even allow you access your device's camera so you can take video or snapshots through a cloud application – talk about red-handed.
- **Disable your wireless (Wi-Fi) connection when you are not actually using your device to connect to the Internet** – better safe than sorry.
- **Bring your charger** – don't charge your devices by plugging into any foreign device. Just plugging into a USB port of a strange device makes you susceptible to malicious software downloads – you don't even have to click on anything, plugging in is enough. Never plug in or load any foreign media – everything from USB sticks and flash drives, to CDs and DVDs, can leave you infected with malware.
- **Contact Details** – whether you make a wallpaper screen or include a handwritten note, make sure your local contact information is with your device so it can be returned if someone finds it – yes, it does happen, especially password protected devices.

For any information security concerns, contact the Information Security Team at itsecurity@uthsc.edu or (901)-448-1579.