CLOUD AND BASIC CYBER SECURITY AWARENESS

Simple steps on how to use
the Cloud securely and how to keep your computer systems secure at work and at home

AGENDA

- Introduction
- Using The Cloud Securely
- Four Steps to Staying Secure
- Questions

INTRODUCTION

- Homeland Security: October 2016 was the National Cyber Security Awareness Month
- We live in a world that is more connected than ever before. The Internet touches almost all aspects of everyone's daily life, whether we realize it or not
- Cyber Security Awareness educates computer users to be aware of cybersecurity procedures and to provide them with tools and resources needed to stay safe online, and increase the security of our computers systems and networks at work and at home.

USING THE CLOUD SECURELY

- "The Cloud" is a service provider on the Internet to store and manage your computing systems and/or data for you. We call these services "The Cloud" because you often do not know where your data is physically stored.
- An advantage of the Cloud is that you can easily access and synchronize your data from multiple devices anywhere in the world, and you can also share your information with anyone you want.
- The Cloud is neither good nor evil; it is a tool for getting things done, both at work and at home. However, when you use these services you are handing over your private data to others, and you expect them to keep it both secure and available. As such, you want to be sure you are choosing your Cloud provider wisely.

USING THE CLOUD SECURELY

- For Cloud Service for your personal use, consider the following:
  - **Support:** How easy is it to get help or have a question answered?
  - **Simplicity:** How easy is it to use the service?
  - **Security:** What data is collected about you, if any?
  - **Terms of Service:** Take a moment to review the Terms of Service. Confirm who can access your data and what your legal rights are

USING THE CLOUD SECURELY

- Securing Your Data
  - **Authentication:** Use a strong, unique passphrase to authenticate to your Cloud account.
  - **Sharing Files/Folders:** The Cloud makes it very simple to share, sometimes too simple. The best way to protect yourself is to not share any of your files with anyone by default. Then only allow specific people (or groups of people) access to specific files or folders on a need-to-know basis.
  - **Sharing Files/Folders Using Links:** One common feature of some Cloud services However, this approach has very little security. Anyone that knows this link may have access to your personal files or folders. If you send the link to just one person, that person could share that link with others

USING THE CLOUD SECURELY

- Securing Your Data
  - **Settings:** Understand the security settings offered by your Cloud provider. Find out if there are ways to see who has viewed your shared content and when they viewed it. Make sure you can restrict your shares to "read only" versus giving read+write to people, if they do not need the read+write rights
  - **Antivirus:** Make sure the latest version of antivirus software is installed on your computer and on any other computer used to share your data. If a file you are sharing gets infected, other computers accessing that same file could also get infected.

FOUR STEPS TO STAYING SECURE

- As technology gains a more important role in our lives, it also grows in complexity. However, regardless of what technology you are using or where you are using it, we recommend the following four key steps
  - **You:** Keep in mind that technology alone will never be able to fully protect you. the greatest defense against attackers is you. Be suspicious and by using common sense, you can spot and stop most attacks.
  - **Passwords:** The next step to protecting yourself involves using a strong, unique password or a passphrase for each of your devices and online accounts.

FOUR STEPS TO STAYING SECURE

- **Updating:** Make sure your computers, mobile devices, apps, and anything else connected to the Internet are running the latest software versions. Cyber criminals are constantly looking for new vulnerabilities in the software your devices use. To stay current, simply enable automatic updating whenever possible.
- **Backups:** Sometimes, no matter how careful you are, you may be hacked. If that is the case, often your only option to ensure your computer or mobile device is free of malware is to fully wipe it and rebuild it from scratch. We recommend you store your backups in either the Cloud or offline to protect them against cyber attackers.

QUESTIONS?

THANK YOU!