Tips on Securing Your Communications

The following best practices are being offered for general reference only and readers should consult with their Information Technology departments for specific guidance.

Cyber security threats regularly impact individuals on their corporate and personal devices and a heightened level of security and awareness is necessary on both personal and corporate devices. As employees increasingly participate in corporate Bring Your Own Device programs, the line is blurred between personal and corporate communications as corporate data is regularly accessed through or moving across personal devices. The following list of industry best practices is not an exhaustive list but may help reduce your risk of infection.

On Personal Devices:

- Ensure you access corporate data using only those security tools implemented by your organization. Do not circumvent these tools by using webmail or connecting to the corporate network outside of a secure connection. Do not store sensitive corporate information on personal devices. Whenever possible, promote separation between resources used for work and personal matters.

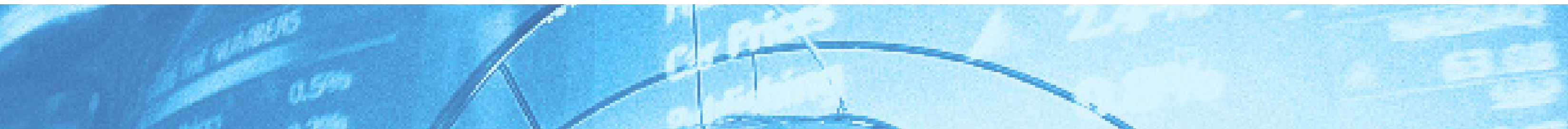
- Avoid using free public Wi-Fi connections. If this is unavoidable consider using a commercially available VPN solution on your personally-owned computer and mobile devices to prevent the capture of your data stream.

- Exercise extreme vigilance when clicking on any links or opening attachments. If any of the following elements are out of the ordinary, do not click on the link or open the attachment – time sent, minor variations in the email address, file name, or actual web address of the link embedded in the email. In the event that you do click on a suspicious link or attachment do not use the device until you run a virus scan and perform any necessary clean up recommendations.

- Regularly follow these steps to ensure that your personal devices are secure:

  - Update the mobile device/laptop operating system when told to do so by system update messages

  - Ensure that you are using an Internet browser that is updated



  - Pay attention to pop-up alerts while browsing and do not grant security exceptions, particularly for expired certificates, or bypass security notifications and warnings

  - Laptops should include a commercially-available anti-virus solution that is regularly updated

  - Make sure that encryption is being used (HTTPS in the address bar) when inputting any user names and passwords; if you are unsure if encryption is deployed in an application, use a commercially available and reputable VPN provider

- All devices should be password protected, using a complex and unique password. While traveling, try to keep any personally owned mobile devices or laptops in your possession or in the physical possession of a colleague. Avoid leaving devices unaccompanied in hotel rooms, even in locked safes. When traveling abroad, avoid authorizing system updates as these may be fraudulent alerts sent when you connect to a hotel Wi-Fi service.

- Research and confirm the legitimacy of any application that you authorize to be installed on your personal device. Malicious applications circulate widely and can capture all of your keystrokes and even data stored on your device.

On Social Networking Sites (SNSs):

- Regularly change passwords and ensure that passwords are not duplicated on multiple SNSs or other sensitive platforms such as corporate accounts, bank accounts, and personal email accounts.
- Enable multi-factor authentication, when available. This feature is oftentimes offered by popular SNSs; however the user must elect to activate the feature. This can be found in the SNS help tab or search bar.
- Be vigilant of connection requests from users, even those with established connections to family or friends within your network. Fraudsters posing as legitimate contacts are active online.
- Maintain familiarity with the privacy filters and rules to ensure awareness of how your content is being shared. Changes are frequently made by the SNSs, requiring periodic attention by the user to the settings. Set your privacy filters at the highest levels.
- Exercise caution when clicking on links sent by email, especially shortened URLs, when on an SNS. This is a prime mechanism to infect a machine with malware. To access the site, go to a new tab and type the name of the site into the address bar; do not cut and paste the URL.
- Avoid clicking on any links within emails or opening unexpected attachments, particularly when the emails are branded with your SNS logo. Instead, login to the SNS directly via the URL. The quality of fake SNS sites are difficult to discern from the real SNS site, which tricks users into providing personal information after clicking a link to connect with the SNS site.