Protecting personal information–A day in the life

Morning commute 7-9am

Opening emails
Checking email from your phone can sometimes be dangerous, as you may not be able to see the full Sender information. If you don't know the source, don't open it. If you suspect something may be malicious, e.g. Phishing, when you get into the office, report it to your IT support team ASAP or report it through the Report Phishing button on your screen.

Talking
Watch what you're saying and how loudly you're speaking. There could be people listening nearby who could overhear any sensitive discussions that may include personal information.

Using your mobile-device for emails
Checking to make sure e-mail addresses, contents and attachments are correct before you send is hard to do on mobile devices. Consider waiting until you get to the office. If it can't wait, make sure you're using your company's e-mail system.

At the office 9-5pm

Downloading things
When you're working, you could discover a third-party app, browser or IT system you like and feel compelled to sign up for or download it to potentially improve a business process. All software requirements (installs and web-based applications) should first be vetted with your IT support team to avoid introducing malware or other complications.

Sending secure emails from the office
Only use your company's official e-mail system to ensure e-mails are viewed and sent securely, and that any additional controls (e.g. virus checking, malware screening, activity monitoring) aren't accidentally bypassed. Follow your company's IT security policies for guidance on screen-locks, password protection and storage encryption.

Seeing personal or sensitive information
Have you seen personal or sensitive information? Ensure the data is secured. Refrain from sharing it further unless there is a justified business reason.

Transferring personal information
About to send data to a third party? Wait until you are positive your company has a contract or signed NDA. If transferring files to an approved third party, use a secure file transfer solution when sharing sensitive information.

Purging or archiving outdated files
Have old files or reports? Archive or delete them as appropriate if no longer needed. Check with your IT support team for guidance on approved local processes, including any Document Retention, Marking and Destruction policies.

Evening commute 5-7pm

Leaving information unattended
Be careful not to leave your laptop open or PC screen visible. Remember to lock your system screens, when leaving them unattended in the office, and shut down your computer fully at the end of the day before heading home.

Taking something out of the office
You may need to take data out of the office when you work from home or go on a business trip, particularly if it's housed on your laptop. Don't be careless with data, no matter where you're managing it from. Everything from a USB stick to a folder should continue to be managed in line with your company's normal processes.

Disposing of confidential data
Don't leave sensitive or confidential papers lying around (such as on a train or elsewhere)–be sure to lock them away or, if you don't need them anymore, shred them or put them in a secure locked shredding bin.

Going online
On the evening stop at the local coffee shop, think twice before connecting to non-secure WiFi networks. If you're planning to access personal information, always use a VPN (Virtual Private Network) that encrypts data even if it is flowing through a potentially secured network.