Expert Advice

with Rick Mislan '91

Rick Mislan '91 (professional and technical communications) is currently serving in the newly created computing security department within the Golisano College of Computing and Information Sciences. Before that, Mislan was a professor in Purdue University's College of Technology and was a Communications Electronic Warfare Officer for the U.S. Army.

Security in the palm of your hands

As mobile phones continue to permeate our personal and professional lives, there is a growing need for better mobile security. Currently in the United States, there are more mobile phones in use than there are people, and that number will continue to rise. As the ultimate human-computer interface of the 21st century, our mobile phones help us transcend space and time through multiple communication, transaction and entertainment tools. As we continue to use these mobile tools to organize our personal and professional lives, more and more of our personal and professional data increasingly becomes at risk. To that end, there is an increasing need to secure your mobile device from prying eyes. The following is a list of suggestions to help keep your data protected and private.

1. Install anti-virus software

While there is no one single solution for protecting your mobile phone from being infected by a virus or other form of malware, some protection is better than none. Make sure you install one of the more popular anti-virus suites for mobile devices like those provided by Lookout, McAfee or Symantec. Each of these offers various levels of protection and a few even provide information backup and lost device location services.

2. Use a password

While having all of your personal and professional contacts, family photos and social media

accounts all accessible from a single device is a great convenience, it can also be a great data risk. If you ever lose it, have it stolen or just leave it behind in an office or plane, your only hope for privacy is a secure password. However, the big tradeoff in securing that information with a password is the inconvenience of having to enter a password every time you want to look at the screen of your phone. For the occasional user, this may not be a concern, but for those who check their phone frequently, entering a password or unlock code every time quickly becomes a nuisance. Determine what you're willing to give up if your phone should become lost or stolen. If it's not that important, then you may not need a password. But if the information stored on your phone is particularly sensitive, then use a strong password or download an app that can help provide more layers of protection.

3. Be careful what you click

As our mobile phones are becoming smarter, in terms of what they have access to and what they provide, there are many more opportunities (email, text messaging, images, QR codes) to provide links to the Internet. The problem is that many times those links aren't friendly and could be phishing you for your personal information. Specifically on mobile phones, there's not always an easy way to verify the link or ensure the picture is not a virus before you click to view the image. Only click a link or image if you are sure it is legitimate. Remember, if it smells phishy, it probably is.

4. Location, location, location

One of the many features of the smartphone is the location service through the Global Positioning System or through WiFi. While it is useful to pull up a map to see what's available around you, it is that location service that will also define where you are currently located. While immediately useful to you in finding the nearest coffee shop, it is also possibly detrimental to your personal safety as many smartphone apps have access to these location services for no apparent reason and can provide it to some other person or group. Location data also finds its way in the images you take with your smartphone camera. Known as Exchangeable Image File data, hidden geographical identification information stored in your image files can provide a relatively accurate latitude and longitude. So use the location services only when necessary; your battery will thank you as well.

5. Know your apps.

Increasingly, as we install apps such as Angry Birds and Words with Friends, we think we are selecting seemingly safe apps. These apps may have no need for your personal contacts but will actually have complete access to them while you are playing the game or using the app. When agreeing to install an app and all that it does for you, the acceptance click is your best chance to restrict the applications' access to your personal information. Select only the options you wish to provide, keeping in mind that the app may not work as well as intended after you've restricted a few of these items.