Information Technology (IT) Security Guide

A digital safety guide to protecting you and your work

Mobile Phone Safety

These days our mobile devices are used as much or more than our computers. With the functionality they now have, there is often valuable information on them. Tablets and mobile phones should **always** be protected with a password or PIN that locks automatically after two to five minutes without use. If possible, set your phone to automatically wipe all data after 10 incorrect password attempts.

Be aware that **mobile phone conversations are easily monitored** and many modern phones are trackable. If your location could endanger you and others, you can disable tracking abilities by turning your phone off completely and removing the battery if possible.

Avoid using text messages (SMS) to send or receive sensitive information since this information is more likely to be intercepted or compromised.

Instead of sharing information over mobile networks, computer-based phones such as **Jitsi** are much better ways to communicate privately. You can get Jitsi for free at: www.jitsi.org. Jitsi uses a ZRT protocol for encrypting data. However, this is no replacement for common sense. Please refer to the Jitsi FAQ to understand the technology and confirm that the security is working properly: https://jitsi.org/index.php/Documentation/ZrtpFAQ

Keep careful track of SIM cards. Someone could use the personal data stored on them to impersonate you.

PC Protection

Strong passwords

The easiest way to secure your information is to **create strong passwords**. Your passwords should have at least eight characters combining symbols, numbers, and upper & lowercase letters. A good tip is to start with a sentence, remove the spaces, intentionally misspell some of the words and add numbers at the end. The following link from Microsoft has advice on how to create strong passwords: http://www.microsoft.com/security/online-privacy/passwords-create.aspx

Remember to change your passwords *at least* once every three months, and be sure that the lockout on your computer is set to 5 minutes or less. Also be sure to password lock ***ALL*** digital devices, especially your PC, phone, and Wi-Fi. Never write down your passwords or give them to anyone. Use equally strong passwords for online accounts and email.

Stay Virus Free

The internet is a dirty place, but it's easy to stay clean…

Almost everywhere you go online can expose your computer or mobile phone to viruses that can damage and steal your information. It is critical to have strong antivirus software running on your PC at all times. Fortunately, there is software available that is both very good and completely free, called Microsoft Security Essentials. It is available at: http://windows.microsoft.com/en-us/windows/security-essentials-download. If you are using Mac products, free Sophos anti-virus tools are available at: http://www.sophos.com/en-us/products/free-tools.aspx.
After you've installed antivirus software, continue to safeguard your computer in four easy steps:

1. Always **avoid clicking on ads** and unknown links.
2. **Never download files from unknown sites** or open email attachments from someone you don't know.
3. **Don't use unknown flash drives or discs**.
4. **Save all files to a folder first** rather than clicking directly. Then, open the document from inside a program such as Word or Excel.

Security Begins With Your Awareness

The first step in data safety is to make sure your computer and other devices are kept out of the wrong hands. Always keep your laptop and other portable devices containing your sensitive information in a safe, secure place when not in use.

While Traveling
Keep devices with you at all times and out of sight as much as possible. Never show your equipment to anyone unnecessarily, as you don't know who else might be watching. Avoid using or discussing devices in public places or in front of people you don't know.

When in the Office
Always lock away equipment in secure spaces, out of plain sight. If an intruder can physically get to a server or computer, they could install a virus or tracking tool that could report your information and activities back to them. When at your desk, be aware of the direction your screen faces, keeping in mind that someone might be able to read your screen if positioned the wrong way. As a best practice, it's wise to keep your computer and desk faced away from others in the office and open windows on the ground floor. Most computers also have a slot where you can route a locking security cable. If your office is shared or has public traffic in and out, it's a good idea to get such a cable and lock your computer to your desk to prevent theft.

Email etiquette and security
Use BCC when emailing a distribution list. This helps the readers, since he or she does not have to scroll down to read the content. In certain instances, it is also good security since all recipients are hidden and could not be traced back to any sensitive themes or topics.

Wi-Fi Access
While wireless access points are convenient, without the correct security settings, they can compromise your network and data. When setting up your wireless router, turn on Wi-Fi Protected Access (WPA or WPA2) encryption with a strong password so unknown persons cannot join your network. Never share the password with outsiders. If you have frequent guest users, consider creating a guest-only login that is not connected to your network or any work computers. To learn how to set up a secure Wi-Fi, please visit this online tutorial: http://www.wi-fi.org/discover-and-learn/security

Safe Web Surfing
"HTTP" OR "HTTPS," the letters at the beginning of every web address, stand for the way information is passed back and forth between a website and visitors. The "S" at the end stands for "secure," meaning that this page is encrypted. When you look at the URL in the web browser, it will likely begin with just http://. This means that the site is talking to your computer using 'insecure' language. In other words, it is possible for someone to eavesdrop on your interaction with that website. However, if the web address begins with https://, your computer is talking to a secure site that ensures privacy. Although a website has the "s," that does not always mean it is safe to interact with — even scammers can have secure sites! It simply means that no outsiders can listen in. Communicate only with reputable organizations and websites you know are safe.

Secure Communications
There are different levels of communications security depending on the type of encryption a tool uses. Tools that provide end-to-end encryption (such a PGP-encrypted email, or chat with OTR or Textsecure or CryptoCat on your phone) are more secure than tools such as Gmail, Facebook, or Twitter that use transport-layer encryption. Mail, phones and text messages (unencrypted) are the least secure. Choose the most secure tool you can given your available resources. In many cases, it is better to reach out for help insecurely than not to reach out for help at all.

Taking it to the Clouds: Backing Up Your Data

"There are only two types of hard drives- the ones that have failed and the ones that will fail."

Since computer hard drives aren't always reliable and can be stolen, **always keep multiple copies of all your files in two different places.**

An internet-based "cloud" service is a great option for making sure your files stay backed up. There are many **free services available** online such as DropBox, Google CloudDrive, Box.com, or Amazon Cloud.

Cloud backups are a safe method of storing your data because they are encrypted (use https) and kept safe in a remote location, allowing you access to your files even if your computer is stolen or destroyed. If cloud storage isn't possible, use an **encrypted flash drive** to make a backup copy of all your files. Keep it in a secure location whenever you can.

Developed by Alexandre Carle, OTHER SOLUTIONS Consulting, acarle@othersolutions.eu, Katie Skartvedt, Catherine H. Townsend and Carlos Velez,