RCM&D

Assurex GLOBAL | Private Client Practice Group

# Cybersecurity Privacy and Security:

## Important tips and considerations while on the web

**LIKE A THIEF CUTS THROUGH A BIKE LOCK,** hackers can override your technology's security measures. To keep us mindful of security best practices, Assurex Global's "go to" resource for digital forensics and cybersecurity, LIFARS, has answered questions we should all be asking.

## Computers

Although we often take work home, we should not use our personal devices for work or vice versa.

### Can I use my work laptop at home?

Unfortunately, using a work laptop at home can be risky for both you and your business. This practice has led to many security incidents that have resulted in the loss of confidential data and financial damage. Why? Quite often, workplace laptops are set up to access company data, files and accounts automatically—making these files easily available should your work device become compromised.

### Can I use my home laptop for work?

The dangers also apply to using personal computers for work purposes. Many gaming, entertainment, and adult websites that are blocked at work are available for use at home. These sites are hotbeds for malware. So, if anybody in your house uses these entertainment sites, and you use the same computer for work, hackers may easily get the information they need to compromise the security of your business information.

## Home Security Systems

It might seem unnecessary to secure an in-home security system, but this assumption could compromise your home security, personal belongings, and your online data.

### How can there be risk in using a security system?

Recent reports suggest that hackers can access the technology used within in-home security, giving the attacker unauthorized access to your personal data and the opportunity to rob your home.

JANUARY, 2015. ISSUE 2

ASSUREX GLOBAL QUARTERLY SECURITY UPDATE: PROVIDED IN COLLABORATION WITH LIFARS

**How can I secure my in-home security systems?**

In many cases, the mistake people make is very basic: they don't change the default password. This seems trivial, but thousands of people's home camera systems can be publicly accessed via online portals through this one mistake.

The most popular wireless home alarm systems may contain flaws that allow criminals to disable the alarm. To be completely safe, it is recommended that you use a wired system rather than a wireless one.

## Mobile Devices

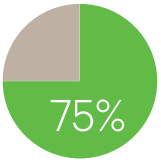
Today, losing your smartphone, tablet, or even your smart watch is a risk. These devices have become the gateway to our lives, making their security critically important.

**What are some steps I can take to keep my information safe?**

1. **Set up a lock by creating a PIN or a fingerprint scan.** This form of security makes it much harder for others to access your lost or stolen devices. We do not recommend other methods of security, like face detection or patterns, as they are easily circumvented.
2. **Encrypt your device and the data on it.** Encryption makes it nearly impossible for any unauthorized user to access private information. Since the encryption steps are different for every device, contact customer service or visit the official website to find out how.
3. **Make sure your software is up to date.** You can do this through the settings or the Play Store/App Store. This will ensure that your software does not have any known security holes.
4. **Use mobile data instead of public Wi-Fi.** Public Wi-Fi, especially a free hotspot, is commonly hacked and can be used to take all of the traffic transferred. If you do not have a choice and need to use a public hotspot, do not access your bank accounts, work, or social media accounts. Turn off form autofill and do not use the option to remember passwords.
5. **Install anti-virus software.** This will help protect your device from viruses. Many anti-viruses also feature a tracking and remote disable feature that is invaluable in the case that your device is lost.

## Social Media

Around 75 percent of adults use social networking sites, giving hackers a large pool of potential victims.[1]




**use social networking sites**

### How can I ensure my information is private?

Many social media sites offer privacy control over who can see your content. Use them. Do not share unnecessary information on social media as it can be used against you. Also, no matter what your privacy settings, be judicious in publishing information about your location and activities taking you outside the home.

## Email

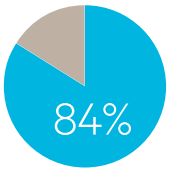
Humanity sends around 200 billion emails per day.[2] That's a lot of opportunities for hackers to steal information.

### What are some ways to keep my email private?

Use a trusted email provider, such as Microsoft Outlook, Yahoo Mail, or Gmail, as these providers have strong security and a high quality spam filter. You should also create a secondary "spam" email address and use it when signing up for services and when opening accounts on new websites (those from which you do not want to receive promotional email). This will prevent spam emails from reaching your primary mailbox.

## Internet Browsing

Nearly all—84 percent—of U.S. adults use the Internet.[3] But, just because almost everyone browses online doesn't make it safe.




**of U.S. adults use the internet**

### Is my private information secure when browsing the Internet?

No, it is important to remember that anything "free" on the Internet is not actually free. Your browsing records are often traded for your privacy and used for various purposes, such as tracking and target marketing.

Only give your data to websites that you trust, and only if you know that there is a secure Internet connection. You can verify security by checking to see if the lock icon is at the top of your web browser and/or in the pop-up box where you are entering data.

[1]Pew Research Center. "Social Media Usage: 2005-2015." http://www.pewinternet.org/20
[2]The Radicati Group, Inc. "Email Statistics Report, 2014-2018". http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf15/10/08/social-networking-usage-2005-2015/
[3]Pew Research Center. "Americans' Internet Access" http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/

LIFARS
your digital world, secured

LIFARS is a digital forensics and cybersecurity intelligence firm based in New York City. Our incident response and penetration testing teams consist of the top experts in the field. As a testament to our excellence, LIFARS was ranked the #2 cybersecurity company in New York Metro area on the Cybersecurity 500 list of the hottest and most innovative cyber security companies.

Assurex GLOBAL | Private Client Practice Group

Founded in 2014, the Private Client Practice Group assists Partner firms to collectively leverage their resources and industry influence to better meet the personal protection needs of high net worth clients. Through this Group, our Partners are able to provide their private clients with access to proprietary insurance solutions, specialty programs, and the collective thought leadership that can only be achieved in a culture of collaboration among best in class personal risk advisors.

JANUARY, 2015. ISSUE 2

ASSUREX GLOBAL QUARTERLY SECURITY UPDATE: PROVIDED IN COLLABORATION WITH LIFARS