Security
Spotlight
An informational Guide for Securitas Canada Clients and Employees

January 2016 | Securitas Canada Limited | Number 142

Ten New Year's Security and Safety Resolutions

As we begin the New Year of 2016 we should use this time to clean the slate and start fresh. Most people use the start of a new year to make some type of resolution and we, here at Securitas Canada, encourage you to further that by making your resolutions with a security focus. It is necessary that we are placing proper attention on ensuring that we are re-examining our safety both in the digital and physical spheres. These resolutions should be applied at least once a year and be a reminder that this is an on-going process.

ELECTRONIC SAFETY

We live in a digital world and are reliant upon the use and interaction with technology both for professional and social aspects. It is important for us to safe guard our electronic world from would be thieves, hackers, and those that operate in the online shadows. There are five important items that you should resolve to complete as part of a New Years' resolution in security.

First, reset your passwords for all digital logins. Though this may seem daunting and tedious, it ensures that you are proactively staying one step ahead of would be criminals. This includes email, any website logins, your mobile phone screen lock, and even home and office security codes.

Second, check your social media privacy settings. Since social media applications are constantly evolving those companies do make changes to their programs and can, in the course of an update, open your "private" information to public view.

Third, Learn about the latest online scams and what you should know to ensure safe electronic communications and Internet browsing. Phishing is a general term for e-mails, text messages and websites fabricated and sent by criminals and designed to look like they come from well-known and trusted businesses, financial institutions and government agencies in an attempt to collect personal, financial and sensitive information. It's also known as brand spoofing (RCMP 2015). Ensure that all of your electronics software, anti-spyware and malware are up-to-date. You do not want to be out-of-date because this will lessen your electronic protections and increase the chances of an attack, hack, or virus. Remember, this should include any and all computers, tablets, mobile phones, and GPS systems. Be suspicious of any e-mail or text message containing urgent requests for personal or financial information (financial institutions and credit card companies normally will not use e-mail to confirm an existing client's information). As a general rule, do not open, forward or otherwise click on anything in emails that are suspicious or that came unexpectedly (even if it's from a vendor or a contact). Be suspicious of zip files within emails. Remember, seeing your name or email address anywhere in the email body does not mean it is legitimate. If you suspect your computer has been infected, do not connect to your company/home network. Unplug the network cable and switch off or disable your wi-fi connection. Report it to your network administrator immediately.

Fourth, backup all of your electronic files. Both industry and federal agencies suggest this course of action. It does not matter whether it is to the cloud or on some type of hard drive, having a copy of the files can protect you financially and professionally. Security experts recommend the 3-2-1 format: three copies, two different formats, and one off-site. This will also ensure that should the need arise you have multiple formats from which to access the saved information (IM Basics – Government of Canada 2015).

Fifth, when you are out of the office or leaving for the day, turn off your computer. This will ensure that no one is remotely accessing your computer from the internet. Also, in this strand of thinking, have your computer set to lock the screen if it is idle for more than two minutes. This way, if you walk away from your desk or work station, no one can come and access your computer and sensitive files contained within it.

WORKPLACE SAFETY

Now that we have focused upon the digital domain, let's examine the physical aspect of safety at our workplace. It is important to realize that there are small steps one can take to improve our understanding of potential threats that exist in the office setting. In examining our New Years' resolutions there are five steps one can take to increase their physical safety.

First, check your understanding of your company's emergency exit plans and site evacuation alarm system. Understand the types of action plans and responses company employees should follow. Also, be aware if varying incidents will require different responses. An example would be a reported fire compared to a bomb threat. Also, know if there is a rally point to meet outside of the building, if an emergency event requires the evacuation of the entire site. If there is a rally point, practice an actual evacuation for a recommended yearly building clearing to make sure everyone knows what to do and where to go.

Second, re-evaluate your routine when entering and leaving work. Use the main entrance and avoid rear or secluded exits. Always be cautious and aware of your surroundings when walking in a parking lot. Vary your routine, routes, and times to make sure you're not predictable. Always try to park in well-lit areas and not next to large vehicles that block your view. Think about a buddy system or safety walks to your automobile. Do not unlock your vehicle remotely until you are next to the vehicle and immediately lock the doors and keep the windows rolled up until moving. Always look into the vehicle if left unlocked before entering it to make sure no one is hiding in the back seat. Criminals do target parking lots and garages because there are many places to hide and provide relative ease in escape after committing a crime.

Third, lock your office door or desk drawers in your cubicle each and every time you step away from your area. At minimum, do it when you will either be away for an extended period of time or for the rest of the day. This simple act will lower the chances or at best create a deterrent for a dishonest co-worker or outside vendor from rummaging through your desk drawers looking for items of value.

Fourth, secure hard copies of documents and other sensitive corporate materials. In the modern day of corporate espionage, protecting internal company items is important to maintaining an edge in business. Also, if files were to be stolen, it could have an indirect negative effect leading to loss of business and forcing a company's management to lay off employees.

Fifth, re-familiarize yourself with the visitor policies of your company. Knowing who is a visitor or vendor and where they are allowed to operate will protect everyone. Also, know who should have access to sensitive sections of the building. Furthermore, never allow anyone to piggy back off your entry into the building. If you observe another person attempting to enter the facility in this manner, always ask them for their company identification, if it is not visible. By knowing what the policies and the type of identification badge system your company has established, it will enable you to be more aware and protect your company from theft and potential threats.

CONCLUSIONS

Securitas Canada wants to wish you a Happy New Year and reminds you that the value of Vigilance must constantly be rekindled. It is through this proactive approach and assessment of our electronic and workplace security that we can stay protected and secure throughout this coming year. ***Here's to a safe and happy 2016!!***