FORT SHERMAN ACADEMY

Providing Traveler Safety Training and Risk Management Services

Topics in this edition:

Spring 2018 Newsletter

Beware of Ransomware

Encrypt? Really?

Trending Scams

New Course!

Ransomware is Spreading

The growth in ransomware at the personal level was probably the most notable security event of this past year, with losses tallying over $1 billion. 2017 saw a huge increase in this crime, which involves the victim unintentionally installing malware on their computer and then being denied access to their data until a ransom is paid.

It should not be a surprise that hackers are continuously discovering new ways of tricking people into downloading this type of software, evidenced by the fact that ransomware was found in almost two-thirds of malicious emails in late 2017. What is surprising is that people are still not safeguarding their computers and data and therefore are forced to pay hackers for their files.

Back up your data – Use a system that backs up your files automatically. That way if you're nailed with ransomware, you'll have the opportunity of restoring the data.

Keep the software updated – This means set your computer and software (antivirus, antimalware, firewall) to update automatically. Truly, this is the most critical step you can take to improve security.

Check those links before you click – Hover over the suspicious link title and the full address will appear. If you recognize it, great. If not, verify its safety with SiteCheck.Sucuri or Urlvoid. While not perfect, it's a huge step in the right direction.

Are You Ready to Lose Your Laptop?

The Department of Homeland Security is again considering extending a ban on laptops and tablets in carry-on luggage to all US – bound flights from Europe. DHS says that terrorists may try to conceal bombs in these devices. This ban means that travelers would have to check their laptops at the airport, which obviously raises concerns for those with sensitive information. Whether it's a human resources file or photos of their children, nobody wants data getting accessed by a hacker if the laptop is lost or stolen.

Option 1: International travelers can buy a cheap second laptop, store the data they need in the cloud, and then access it once they get to their destination. Before getting back on the plane for the return flight, wipe the data.

Option 2: Encrypt your laptop's hard drive. Full-disk encryption makes all of your software and data unreadable unless you enter a passphrase. Once done, it works automatically, and any new data you save on your laptop will also be protected. Even if someone actually removes the hard drive, it will be unreadable.

Remember, setting a simple screen lock on your laptop is a much weaker level of protection, one that can be sidestepped by hackers. So, set up full-disk encryption with *BitLocker*, *FileVault*, *VeraCrypt,* or the like and utilize a long, strong passphrase. Finally, power it down. "Sleep mode" leaves the drive decrypted and accessible.

Trending Scams

~ A “friendly” national or English-learning student offers to show a tourist around town and then invites him/her to enjoy food or drink at a nearby local teahouse or restaurant. The visitor is taken to a dimly lit back room and given a menu with small print. Sometimes, the beverages are spiked with drugs to impair vision and/or judgment. When the bill arrives, the host leaves and the establishment intimidates the visitor to pay an exorbitant bill or face assault.

Advice: Avoid being led around by an unplanned encounter. Recognize the “friendly” tactic and be aware of your surroundings. Whenever possible, travel in small groups to assist each other.

~ A young “art student” (or rug salesman) will approach and ask if the tourist likes artistic work created by local students. The student entices the tourist to view the work at a studio or gallery where they pour tea and provide snacks as they present their art. The student then pressures the visitor to buy the pieces and demands payment for the hospitality shown.

Advice: Don’t feel obligated to buy or provide something when faced with a “friendly and helpful” salesperson. Remember it’s a technique that makes you feel compelled to follow, especially when you are alone.

New Course for Churches Concerned with Safety

This one-day seminar provides instruction and functional approaches to protecting our churches in a world where church-involved incidents of abuse, theft, and violence continue to spread and increase in occurrence.

Through a biblical view of security management, you will learn how to identify common legal and civil risk exposures, strategies to assess and mitigate soft target areas in your church facility, and the biblical models and authorities for being prudent and setting a guard.

We will also examine and discuss critical areas in developing and training a safety team like: key techniques in verbal de-escalation, best practices in active shooter incidents, and crucial steps in traumatic first aid.

Register now for these CAPTIVE SAINT classes:

B+ May 10 – 11 (ID)

C+ June 12 – 21 Urban (ID)

Register Online

FORTSHERMAN.ORG

C+ July 10 – 19 Rural (ID)

C+ July 31 – Aug. 9 Rural (ID)

LIMITED SEATS LEFT!

PO Box 1059
Pinehurst, ID 83850

info@fortsherman.org

888.211.8674

Fort Sherman Academy trains and supports organizations in faith-based security and risk management. We assist in the furtherance of their mission by training them to better avoid, protect and survive potential or actual adverse events thus allowing them to reach every corner of the globe.