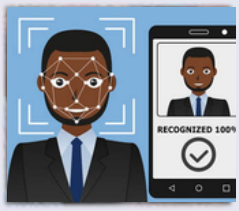
FORT SHERMAN ACADEMY

Providing Traveler Safety Training and Risk Management Services

Topics in this edition:

Fall 2024 Newsletter

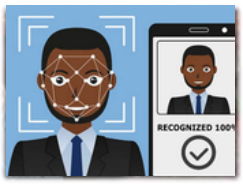


Preventing Phone Tracking

Featured Course!

Trending Scams

IS YOUR FACE BEING USED AGAINST YOU?



In an age where 75% of mobile-device users enable biometrics as their security locks, that convenience has opened the door for government officials to review the contents of your device. In fact, a Federal court has decided that police officers can make you unlock your phone, even by physically forcing you to press your thumb against it. Compared with the common alternative, passwords are much harder for law enforcement to obtain than physical characteristics used for biometric locks such as Face ID and fingerprint readers. That's because biometrics aren't covered by the Fifth Amendment, which protects people from self-incrimination such as giving up a password. (You may remember the case where the FBI was demanding that Apple unlock a suspect's phone.) If you think this is only happening in the US, you are mistaken. Other countries have already followed suit.

How many potentially damaging things do you have on your devices? If you're like most people, the answer is probably zero. Let's look at the bigger picture though. Inflammatory people you call or follow, controversial pictures, products, sermons you have...

Your browser. Email. Facebook. What's App. Dropbox. Signal. The history of everything you've ever searched and everything you've ever said to anyone, is right there in those apps.

Multiple companies now make "forensic software" that can grab all of your photos, contacts—even passwords for your email and social media accounts—in a matter of minutes. Their customers include police agencies of various countries, militaries, and private security forces. All they typically need is an unlocked phone.

By now you should be asking yourself:
1) What am I carrying around with me that I don't need?
2) Did I sign out of all my mobile apps so that they don't automatically open?
3) Should I revert back to a strong password when traveling across borders?

CAPTIVE SAINT - ADVANCED (Level B+)

This two or three-day course involves a comprehensive evaluation of advanced personal protection and captivity survival. It provides pertinent information and provocative interaction for individuals who travel regularly or to increased risk locations. This course provides tools to help in building personal relationships as well as other tools for your toolbox.

This advanced course is specifically focused on adults traveling or working in environments that are at-risk for criminal hostage-taking and illegal government detention. It will also provide skill building for those whose responsibilities include leading teams or responding to teams in crisis situations.

Trending Scams

Watch Out for Scams, After a Disaster Strikes

Opportunities for fraud can occur where there are natural disasters and severe weather. They occur when people may be especially vulnerable, or they target people wanting to help.

Phone, text, mail, email, and even going door to door to target residents of affected areas are tools used by scammers following natural disasters. Here are a couple of things to remember:

- Always verify - Ask the fundraiser for the charity's exact name, website and mailing address so they can independently confirm the information.
- They may use pressure tactics - Scammers often pressure people into making an immediate payment.
- Only give out needed information - Scammers are looking for both money and personal information. Treat personal information like cash and not hand it out to just anyone.
- Question how a donation is requested - Don't work with charities that ask for donations by giving numbers from a gift card or by wiring money.
- U.S. Federal and local disaster workers do not solicit or accept money.
- Talk to people your trust - Before you do anything else, ask trusted people for their advice.
- They contact you out of the blue. If someone prompts immediate action, be cautious.

Look out for these common signs of a scam:

- They ask for your personal information.
- They want you to wire money, pay in cash or purchase prepaid debit cards or request that you make out the check to an individual instead of the business.
- They tell you to keep it secret.
- They make it sound too good to be true. If it seems too good to be true, it probably is!

"It's always better to be cautious than to be a victim."

Contact us to know more about the details and how we can help you meet your safety needs.

Register now for this CAPTIVE SAINT class:

B+ November 12-14, 2024

FORTSHERMAN.ORG

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.