Defensive Strategies

Cyber Safety

By Lyn Bates,
Contributing Editor

What does cyber safety have to do with Defensive Strategies with firearms, the usual subject of this column? I hope you will soon see.

For years I have been a member of NOVA, the National Organization for Victim Assistance. They provide training for people who want to be professional victim advocates. I have been through that training to better help the stalking victims and others I offer help to through AWARE. NOVA provides help to people in crisis due to crime or mass casualties. They also train police about how to respond to situations involving domestic violence, stalking, and similar situations.

NOVA recently offered a full day of continuing education on the subject of cyber safety training just an hour from where I live, so I decided to learn more about the situations stalking victims and others in high risk circumstances ask me about.

The event was hosted by the Rhode Island State Police, so the audience was about half police from varied jurisdictions and half victim service providers. I met local police, police from universities, and an Air Force man tasked with helping his organization deal with its considerable problems regarding crimes against women.

I learned much that I would like to share with you.

Technology has not created any new crimes. Not a single one. Bullying, domestic abuse, elder abuse, harassment, bank fraud, identity theft, identity fraud, stalking and all the sex crimes have been around long before modern technology arrived. There are no new ones to add to the list.

Technology just makes those crimes easier to commit.

One misconception is that you are vulnerable to cybercrime only if you use technology, so staying off computers should keep you safe. Not true. Someone completely off the technology grid can still be victimized, by someone who gets their personal information from a glance at the driver's license in their wallet, from a bank ATM that has been set up to video or otherwise record pin and account numbers of people making withdrawals, or from a stalker who simply follows them home.

More often, you can successfully use technology, from Facebook to smart phones, safely, and in ways that will help foil the criminals out there.

Another misconception is that a "hacker" responsible for cybercrime has to be a computer programmer or someone with a lot of computer skills. Again, not true. Most people responsible for the majority of identity theft have few skills. They have just learned how to use hardware and software easily available on the Internet.

Here's how it can work. A server in a bar or restaurant is paid to use a tiny, palm-held scanner to skim each of the credit cards she or he handles before putting them through the real charge machine. The palm-held device can hold hundreds, if not thousands, of credit card information from that magnetic stripe that makes it work. Every week or so, the identity thief pays off the server, and picks up the collected credit card info by transferring it to his laptop. Then he uses easily found applications to read all the information on each card, change the name and easily purchase hardware to print a new card. Your entire credit card information now has that new name. The hacker will be able to sell those "new" cards with altered names at quite a profit. The old card's information can be altered and new card made in about 5 minutes. I've seen it done.

How else do identity thieves get your data? The leading method is to steal information from government documents, primarily to commit benefits fraud. Credit card fraud is the next most com-

mon, closely followed by medical information and other scams.

What can someone do with a stolen identity? They can use it to try to fool the police. Imagine someone who has enough information about you so that they give that info to cops when they are arrested. Your name and address get on the arrest record. Maybe the person even goes to jail under your identity. Years later, you are trying to get a job in a school, or trying to buy a gun, and the "criminal past" you never knew you had comes to light in a background check.

What else can they do? They can open accounts and buy lots of stuff online.

What else can they do? They can make money illegally. They can set up bank accounts in your name to launder drug money. They can buy and sell online virtually anonymously with your IDand your credit. A huge market is just selling the information they have collected to other criminals. Anyone who has thousands or hundreds of thousands of records from big data breaches can easily find a buyer.

What else can they do? They can target you very specifically. An abusive ex-husband can easily create havoc. One angry ex simply filled out subscription information to nearly 600 magazines with his ex's name and address. It took months for her to realize what had happened, and much work to get it straightened out and her credit corrected.

A year is about average for an individual to recover from identity theft. The feeling of loss of control and power are as powerful with these crimes as any other.

Identity theft is the fastest growing category of crime. Once every 2 seconds, someone is the victim of identity theft in the US. It costs nearly $20 billion a year to fix, and 11% of adults have been victimized in the last year. It can take victims a long time, and a lot of money, to straighten things out.

What counts as "personal information" that identity thieves want to get their hands on? The list is almost endless, but includes your name, date of birth, SSN,

Defensive Strategies

Continued on Page 40

Defensive Strategies

Continued from Page 11

account numbers, passwords, address (even just zip code), banks, credit cards, driver's license number, schools you and your family have been to, jobs, insurance companies, rewards cards, friends and relatives, fingerprints, and all kinds of medical information. It includes all of that information for your family members, too, including ones who have died.

It can take as little as two pieces of personal information to commit cyber crimes.

There are four fundamental principles of cyber safety that you can apply to physical objects and information in electronic form.

The first principle of cyber safety is: You ARE your data. Understand that all those pieces of personal information have real value to criminals, so take steps to protect them. Check your credit reports and Social Security records for you, your minor children and recently deceased relatives. Criminals have been known to open accounts with the stolen identity of children. Those crimes aren't discovered until the child grows up and tries to get credit and discovers that they already have a bad credit history.

Don't use debit cards, ever. They give too much access to your bank account.

Minimize what you carry with you every day to what you absolutely need. If you have to carry a lot, split it up. I carry only a few cards, and now carry medical information and insurance in a place other than my wallet, minimizing the personal information that will go if my wallet is taken.

Personal items with RFID tags embedded, including all US passports being issued now and some credit cards, broadcast their information to any receiver in range. You can foil this by foiling the item, literally. A wrapping of aluminum foil will do the trick, a lot less expensively than a metal-lined passport wallet. Think your cellphone is off? It might still be recording your conversations. Take the battery out, or foil wrap it when you are having really important conversations.

Backup important information frequently. Consider storing it on hard drives or thumb drives in a safe deposit box rather than just on your personal computer.

Most cameras, in smart phones or not, have a "geotagging" feature that embeds the GPS location of the phone as well as the time and date, invisibly in each picture. When you email a photo or post it on a social media site, that location information goes with it, enabling a stalker, for example, to determine exactly when and where that photo was taken. You might want to turn off the geotagging feature.

The second principle is: When asked FOR (personal information), ask what FOR? When asked for some personal information, your date of birth, say, ask "Why do you need that?" "What are you going to do with it" "How will you protect it?" and "What if I don't give it to you?" Many organizations have alternative processes that don't require giving up that sensitive information.

The third principle is: If it has a lock, use it. This applies not just to your home, but to all the accounts you have online. Don't keep your passwords in plain text anywhere on your computer. Long passwords are MUCH more secure than short ones; length is more important than the mix of letters and numbers or capital and lower case letters. Use a password management system like 1Password, KeySave, or the like to protect your passwords, and save you from having to remember them, write them down at home or, worse, carry a written list with you.

Using a fingerprint or line drawing to unlock your phone is much more secure than a typed password that might be overseen (that's called "shoulder-surfing") or guessed.

The fourth principle of cyber safety is: Plan for safety. It costs so much more NOT to pay attention. Don't take any "free offers." The organizations making those offers will be selling your personal info to groups you have no control over.

Update your browsers and operating systems with the newest versions and patches. Running old, unsafe software makes it incredibly easy to be hacked. An appallingly high percentage of computer users have NEVER made these updates. That's like leaving home with your door unlocked and all the windows open—an invitation to be robbed.

Set up online checking and monitoring services to set limits, alerts, and thresholds.

Turn off or disable Bluetooth. Turn off the GPS servings in settings of your apps, except for apps that really need your location.

Be aware when you are deciding for convenience over safety. You might decide to be a little more safe. Use Facebook, but under-

stand and use the privacy settings. Don't friend people you don't know. Think about what personal information you are offering to the world, about yourself and your family. Is it worth the risk?

Google yourself occasionally to see what is out there about you.

For someone fleeing an abusive situation, I would now suggest they get a prepaid credit card instead of just a new card in their own name. Prepaid cards are virtually impossible for an abuser to interfere with. Normal credit cards carry some risk.

Sometimes, a gun is exactly the right tool you need to keep yourself safe. Sometimes, these cyber safety principles and suggestions are exactly what you need to keep your identity safe. Don't make it easy for the bad guys to win in either arena.

W&G

Home Defender

Continued from Page 21

said. "It's pretty much a 50/50 split."

These young mothers often think "smaller is better" when it comes to guns, Esquerre said.

"When that happens, we give her a small gun to fire," he said. "It's small and lightweight, but still fires a 9mm round. She'll say, 'The recoil is too hard,' and 'A semi-auto is too hard to use.'"

At that point, Jolyn gets a standard sized 9mm. Jolyn has arthritis in both hands, but she handles a larger 9mm handgun just fine.

"She shows the student her hands, and teaches her how to rack the gun," Esquerre said. "All of a sudden the student says, 'Oh! That's how you do it!' Then she understands that this isn't a strength thing; it's just learning a technique." From that point on, it gets easier.

"First we have to find her the right gun that makes her comfortable, from a strength standpoint and from a security standpoint," Esquerre said. "Once we get that down, everything starts to flow."

Women who have young children are very safety conscious, Esquerre said. The couple that they're training just decided to go the biometric safe route to keep their firearms away from their children.

"Women are very sensitive to the safety issue, and they want absolute guarantees that their children and their friends are not going to get access to a gun," he said.

Couples learn to shoot from many positions, including flat on the ground.

Esquerre said he and Jolyn train quite a few couples where the woman is the primary defender of the home. Even when that's the case, he said, it's important for the couple to train together so they have a strategy for working together should the unthinkable happen.

"If they train together, they have an understanding of each other's role, and they know how to be supportive of each other," he said. "We've also found that women who get involved with firearms from a self-defense standpoint, whether it's just for the home or just outside, have an awareness that is comprehensive and all-inclusive and covers everything that they do with their lives."

This includes when they're at home or when they go shopping or to work or to their kids' school, Esquerre said.

"Their sense of awareness and alertness and not getting caught in a bad spot is totally expanded," he said. "Once they get good high end training they tend not to become a victim, because they tend to avoid those circumstances or those situations more readily than someone who is unaware and who has never had good training."

W&G