Monthly Cybersecurity Newsletter

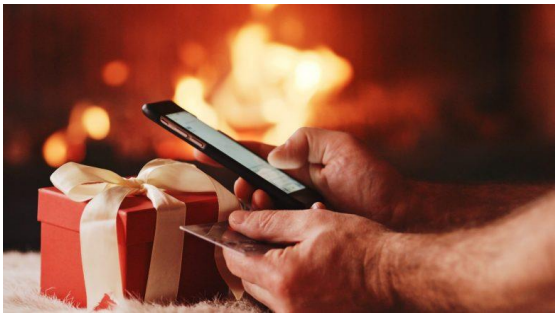
December 2019 Issue

NC DIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

---



7 Ways to Fight Holiday Season Identity Theft

While identity theft can happen to anyone, there are things you can do to reduce your risk. If you think someone is using your personal information to open accounts, file taxes, or make purchases, visit IdentityTheft.gov to report and recover from identity theft. For more resources to protect yourself from identity theft, visit ftc.gov/idtheft. Here are seven simple ways to help protect yourself from identity theft during this holiday season:

- Never use shared computers or public wireless networks for banking or shopping online
- Shred credit and debit receipts and pre-approved credit offers
- Keep a list of all your financial account numbers in a secure place
- Install virus and spyware detection software on your computer and keep it updated
- Never carry your social security number in your wallet or have it printed on your checks
- Instead of clicking on links in emails, type or paste them into your browser window
- Limit the number of credit cards you carry in your wallet

Office Security Tip of the Month

Do you know the difference between ***Piggybacking*** and ***Tailgating***? Both are social engineering techniques used to circumvent physical access controls to gain unauthorized access into a facility. Piggybacking occurs when an unauthorized person walks in through a door behind an authorized employee who has legitimate access and who authorizes the access. Tailgating, on the other hand, though similar, occurs when an unauthorized person walks in through a door behind an authorized employee who has legitimate access; however, the employee does not provide consent and likely has no idea that the unauthorized person came through the door. Employees could be reprimanded or even have their employment terminated for repeated violations of physical access controls. Let's all do our part to protect ourselves, our computer networks and the personal data of the people we serve in our great State.

Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information

Most Americans think their personal data is less secure now, that data collection poses more risks than benefits, and believe it is not possible to go through daily life without being tracked.

According to a Pew Research Center survey, most Americans believe their online and offline activities are being tracked and monitored by companies and the government with some regularity. It's such a common condition of modern life that roughly six-in-ten U.S. adults say they don't think it's possible to go through daily life without having data collected about them by companies or the government. Most also feel they have little or no control over how these entities use their personal information. 70% of adults surveyed say they believe their personal data is less secure than it was five years ago.

But even as the public expresses worry about various aspects of their digital privacy, many Americans acknowledge that they are not always diligent about paying attention to the privacy policies and terms of service they regularly encounter. We should all strive to "Own Our Privacy" by taking action and, as a first step, use these direct links to update your privacy settings on popular devices and online services – privacy settings.

Click here to read the full and unabridged Pew Research Center article by Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner.

WARNING: Cloned Websites

Be wary of all unsolicited emails you receive. It's easy for scammers to clone a website to make it resemble a site you know and trust. They may send you a sale coupon that, when clicked, takes you to a fake website that looks just like the real site. Keep in mind, criminals aren't necessarily looking for your credit card information. The cloned website might simply ask you to log in and then redirect you to the real site so you never realize you were on a cloned page. Once a thief has your login credentials, he or she can access your account to make unauthorized purchases. It's key to make sure the website is legitimate before clicking on it. Those two indicators let you know the site is secure. Also pay attention to the URL address. Cloned site URLs will look like the site they're replicating but aren't really the same. For instance, scammers might use a web address like Amazon-12345.com if they're trying to trick you into thinking they're on Amazon.com.

3 Tips to Protect Against a Home Invasion

By Kevin Creighton

At a Cub Scouts meeting a few years ago, my son and I were tasked with creating a home fire escape plan in order to earn a merit badge. We wrote out what we'd do in case of fire; how to tell if the fire's outside your door and how to move through smoke. We teach fire safety to our children to keep them safe from a fire inside the home, but what do we teach them about how to be safe from violence entering our homes from the outside?

If you look at the floor plan for a typical home, you'll soon see that there are obvious potential points of entry for the bad guys to come in. The plan to secure your home is threefold: secure the exterior, secure the interior, and prepare a refuge.

1. Secure the Exterior

You don't have to live in Fort Knox to be safe, you just have to make your home appear a little more difficult to break into than the home next door. If someone really, *really* wants to get into your home, they're going to, but any casual burglar is going to look for an easy mark to victimize, not a bank vault. So, here are some easy ways to secure the exterior of your home:

Lighting: You don't need to light your home like a prison yard in order to make it safer. I have a simple decorative lighting system in the front yard and some spotlights in strategic locations that light up the dark corners around my house. They make my house look great and also make burglars consider going to another house down the block.

Bushes and shrubs: Consider planting bushes beneath accessible windows in your home that look attractive yet have some thorns and pointy bits that will discourage a crook from entering through that window. Also, keep the other plants in your yard trimmed so they don't provide cover for the crooks as they prepare to enter your home.

Signs: I'm not a big fan of the "I don't dial 911, I dial .357!" type of sign in the yard: Why advertise to crooks there's highly desirable prizes for them (your guns) inside your home? If they know there are guns inside your house, all they have to do is wait until you leave and enter at their leisure. If you have a burglar alarm (more on those later), advertise *that* fact instead: It gives crooks one more reason to move along to another house.

2. Strengthen the Interior

Burglar Alarms: While it's true that the alarm noise probably won't scare a burglar off, an alarm watches over your home when you're not around. Also, an alarm system with a smoke detector can alert you to a fire inside your home when you're not there. The fact is, you can't watch over your house 24/7, but an alarm system can. In addition to all this, an alarm system connected to

your doors and windows can give a few vital seconds to make ready and grab the important gear you need to protect your family.

Exterior Doors: These are a big weakness in most houses or apartments. If your homeowner's association or landlord allows it, consider installing a decorative steel security door or something similar on the front and back doors. If that's not possible, reinforcing the jamb, striker plate and hinges will slow down most break-in attempts to the point where they'll consider giving up and trying something else.

Windows: Are there locks on the windows in your home? Are you using them?

Pets: Dogs have been used as a warning system and theft deterrent for thousands of years, and they perform that role admirably to this very day.

3. Prepare a Refuge

Okay, so now your dog is barking, and the alarm is going off and the bad guys are in your home. What do you do?

At this point, you should get you and your family to a safe place and keep them there until the threat is over and help arrives. Your job isn't to defend your big screen TV; your job is to keep you and your family alive and safe. If the plan for a house fire is to get your family out of the house as quickly and safely as possible, the plan for a home invasion or armed burglary most likely be to get your family into your safe room as quickly as possible. Just as a good fire escape plan has two escape routes for every family member planned out in advance, a good home defense plan has a plan and a backup plan in case that first one fails.

Where should your safe room be? Depends on the home. Remember, time should work in your favor, not the bad guys', so your safe room needs to be somewhere you can get to ahead of the bad guy and hold him off while you wait for help to arrive. Let's examine this floor plan illustration: If this were your home, what area would you designate as a safe room? What are the most-likely break-in points for a home invasion, and where would you and family go to be safe if that happened?

What should your safe room look like? Simply put, it should be more secure than any other room in the house. Make sure the door to the safe room locks and reinforce the door with a heavy-duty striker plate at the very least. If you own firearms, safely store a loaded firearm in the safe room, and team it up with a first aid kit, flashlight and a charged cell phone. Why a cell phone? Any cell phone, in a service plan or not, can call 911 and summon help and having a cell phone dedicated to summoning help in an emergency gives you one less thing to worry about when your life and the lives of your family are on the line.

I realize that this is sobering stuff to think about, but it can happen to anyone. If you have smoke alarms and a fire extinguisher inside your home because you've accepted the fact that fires happen inside the home, you should also realize that your house might be targeted for theft or violence and plan accordingly. Accidents (and crime) happen: It's what we do to prepare for them that determines if there's a successful outcome for us...or the bad guys.

CYBERSECURITY NEWSLETTERS

Security Awareness Newsletter: Monthly security awareness newsletter provided by KnowBe4 for all State employees.
***Note**: You must have a valid State employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month the newsletter covers ***10 Tips to Securely Configure Your New Devices***.

- https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Messaging / Smishing Attacks.***

- https://www.sans.org/security-awareness-training/ouch-newsletter

December 24-26 – State of NC Christmas Holiday

January 1 – New Years Day (State Holiday)

January 20 – Martin Luther King, Jr. Birthday (State Holiday)

January 21 – The Most Devastating Attacks and How to Prevent Them Webcast

January 28 – Data Privacy Day

Be sure to follow DIT on Twitter, Facebook and LinkedIn for more tips. You are also encouraged to review the Stay Safe Online page for additional information and resources on cybersecurity awareness. *Remember…Stop. Think. Connect.*