New Year, New You? Understanding Identity Theft

Wouldn’t it be nice if impersonating someone still required a criminal to change their appearance, falsify intricate government documents, and convince individuals face to face that they are who they claim to be? With all its perks, the amazing convenience of the internet age brings with it the risky reality that impersonating another individual online is easier than ever. With just a small bit of personal information, a hacker can create accounts or make purchases in your name, apply for loans or jobs, get a new cell phone, or even buy a house! Identity theft refers to the deliberate use of someone’s else’s identity for financial gain or for other benefits/resources that come along with an individual’s personal identity. This could include money, assets, a credit rating, credentials to a valuable account, or access to government benefits like a military pension. Until very recently, even modern identity theft required substantial effort, perhaps through time spent dumpster diving for credit card statements; or through superior skill sufficient to hack into a large organization’s database where sensitive information was stored. More recently however, automated hacking tools have made sifting through a sea of information as simple as writing a few lines of code. This reality combined with the rapid increase of information exchange and business conducted online makes each of us significantly more likely to become a victim of identity theft.

In fact, according to the Federal Trade Commission (FTC), approximately 19 people in the US become victims of identity theft every minute! Worse yet, many victims remain unaware their identity has been compromised, giving criminals more time to create fraudulent accounts or incur greater financial damages. Take steps to learn the warning signs of identity theft and be vigilant to protect yourself. After all, there’s only one you in the world, and the ARC Information Security team wants to help you keep it that way! The FTC lists the following warning signs of identity theft:

- You see charges/withdrawals from your bank account that you can’t explain
- Debt collectors call you about debts that aren’t yours
- A health plan won’t cover you because your medical records show a condition you don’t have
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don’t work for
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

The FTC has established a government resource site victims of identity theft. Visit https://identitytheft.gov to learn more.

Better Safe than Sorry! Lessons in Backup & Recovery

Many IT security concepts include complicated technical fixes, intricate code, or expensive software. Others are remarkably simple: make a copy. Failure to back up data commonly results in lost productivity or financial loss. In the Arctic program, failure to backup adequately might mean the loss of important intellectual property, research results gathered over time, or important analysis that could be difficult to repeat. Whether it’s loss of time, money, or just the stress of redoing work, utilizing adequate backups is a best practice that can save individual users and organizations a great deal of frustration. At the organizational level, the Arctic program has policies that advise our IT professionals on how to create and store backups for important systems and how often to update them. Access to backups is regularly tested during Contingency Plan test events. This careful management of data backups at the program level is an example of how the Information Security program seeks to protect the availability of systems that support Arctic research. However, while we can keep systems like the Arctic Research Support and Logistics System (ARSLS) running with adequate backups and backup tests, grantees, researchers, and support personnel are responsible for maintaining their own backups. If your computer failed today, consider what type of data you might lose access to and how that could affect your work. Then, take steps to protect that information. The most important qualities of a good backup practice is backing up regularly, and storing the backup securely and separately from the original. You may consider hardware (such as an external hard drive) or cloud-based backup. The important factors to consider are the amount of space needed for important files and programs, cost of implementing and maintaining the backup, ease of updating/adding files to the backup, and ensuring comparable security (i.e. encryption). Whichever solution suits you best, choosing a backup method is an easy and important way to protect your data and your productivity!
Dell Root Certificate Vulnerability & Repair

During the November session of the Information Assurance Working Group, a member of our team shared valuable information about a recently discovered computer vulnerability that may apply to our readers. Dell Foundation Service, a program installed on many Dell machines that provides automatic security updates, and facilitates customer service repairs, inadvertently introduced a security vulnerability within one of its automatic updates. Left unresolved, the vulnerability may result in transmission of sensitive information about the Dell machine.

Only computers imaged and managed by Dell are at risk of exploitation of this vulnerability. If you use a Dell laptop but it was configured by your organization, it’s unlikely you are at risk. However if you purchased a Dell for personal use, Dell Foundation Service or Dell System Detect may be in use. To prevent exploitation of this critical vulnerability, it is important to follow Dell’s instructions for manual removal of the problematic certificate.

Updated instructions for manually removing the problem certificate are available at http://www.dell.com/support/edellroot. Most end users should not attempt this process without the help of an experienced IT professional. Users may wish to seek support from their home organization’s IT group, or if the laptop is personally owned may visit a commercial IT service operation such as Best Buy’s “Geek Squad” or contact Dell Customer Service.

Up to date information from Dell regarding the problem and solution are available on Dell’s website at http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/11/23/response-to-concerns-regarding-edellroot-certificate.

Holiday Hacks: Exploits in Online Shopping

More users than ever are completing holiday shopping online. Amazon.com reported a record breaking holiday shopping season in 2015, and welcomed three million new members to their Prime service (a membership that includes free shipping on most items), indicating those customers intend to continue making purchases online throughout the year. Of further note, of the millions of holiday purchases made on Amazon this season, nearly 70% of customers made their purchase using a mobile device. It can be assumed that Amazon’s business surge reflects an overall trend toward an increase in not only online shopping, but also in the use of mobile devices to make online purchases. Hoping that the cashier checks ID with credit card payments at the brick and mortar store is no longer a sufficient strategy to protect your credit card information during the holiday season. As a consumer, if you plan to shop online, there’s plenty you can do to protect your information and assets. It can be a real headache to spend time hassling with credit card companies over false charges, and even worse the compromise of credit card information may indicate that your machine or home network have been compromised, putting all of your sensitive information at risk.

If you’re planning to continue shopping online in 2016, and especially if you plan to do so from a mobile device, use the following tips to protect yourself from potential online threats.

- Type website names into the browser yourself as opposed to clicking links. Linked sites may have subtle changes you don’t initially recognize, until you enter your payment information and it’s too late.
- Type the address using https://, and look for a secure logo near the URL like the one picture below. This indicates to you the site is legitimate and information is being transmitted securely.

Always use a credit card instead of a debit card for online purchases. Credit charges are more easily reversed in the event of a fraudulent charge. For additional security, many card companies offer a special feature where each transaction is completed using a one-time use card number so that your real card information is never transmitted. This feature may be advertised as a “virtual number” or “substitute credit card number.” Well established payment sites (such as Paypal.com) are also an option to improve security when paying online, as they reduce the number of times you share your information with another organization. It’s also very important to ensure your Wifi connection is secure. If you’re using public Wifi, wait to make the purchase later or use a trusted Virtual Private Network (VPN) solution to improve the security of your connection before entering payment information.
ARC Program Update: Configuration Management Policy Development

What is IT Security Policy?
Information Security policy sets the foundation of how a business (or in our case, government program) plans to protect information and IT resources such as computers, servers, and network bandwidth. The National Institute for Standards and Technology (NIST) provides guidance for federal agencies on the policies, procedures, and technical controls that must be in place to protect federal government processing standards. NIST divides this guidance into security control families, or categories of information and IT processes. Throughout the year, the Arctic Information Security team reviews the program’s current policy on each control family. Proper policy documentation provides a framework to ensure we’re doing the best possible work to protect Arctic information and assets, while ensuring that Information Security doesn’t interfere with mission requirements. The policy for each control family is reviewed and updated each year. Policy revisions made each year are published program wide in the Information Security Handbook. You can always find an up to date copy of the handbook, along with archived copies of the newsletter, on the Research Support and Logistics resources page at http://www.nsf.gov/geo/plr/arctic/res_log_sup.jsp.

What is Configuration Management?
Configuration Management consists of two main goals. First, establishing a baseline; and second, managing changes. A baseline is an understanding or documented snapshot of how a system normally operates, or an understanding of how IT assets currently operate. Configuration management ensures that any changes made from the baseline are evaluated for operational and security implications, and only approved changes are implemented.

ARC Configuration Management Policy
This December, the ARC Information Security team authored an update to the program Configuration Management Policy. The updated policy includes guidance for the secure configuration of Arctic Information Systems. The primary goal of the policy is to provide a foundation for future development of system-specific configuration management plans. Maintaining detailed configuration management plans wherever possible is an IT best practice that ensures the ARC program is compliant with federal policy and protects the integrity of program IT resources.

ARC IT Spotlight: Maria Petrie, ARC Information Security Team

Have you ever wondered who’s behind the ARC Information Security Newsletter? For this month’s ARC IT Spotlight, I’m including a feature of yours truly, Maria Petrie: Information Security Analyst for the ARC program and author of the ARC Information Security Newsletter. For this feature, I’ll provide responses to the very same questions I’ve asked many of you.

Q: How did you come to support the ARC program?
A: I’ve spent 7 years providing information assurance support to federal clients in both civil and defense markets. My primary expertise is in policy development and audit preparation, so when the NSF Division of Polar Programs had a need for an Information Assurance resource comfortable with a wide variety of Information Assurance support tasks, I threw my hat in the ring for the job. I was most excited about the opportunity to build a foundation of policies and procedures for the program to help document the great work we’re already doing, as well as provide strategies for how we can improve our preparedness for potential information security incidents.

Q: You recently traveled to Alaska for the first time to support the program, how was the trip?
A: Our team is filled with fantastic hosts! Born and raised in the southeast, I had never experienced a climate quite like the one in Alaska. I don’t think I’ve ever been that cold, but I loved every minute! I truly enjoyed getting to see the sites where our teams do their work everyday, getting to know the team on the ground at each Alaska site, and seeing the beautiful state that many of you call home.