Long Distance Robbery

Our main topic at the June meeting was hacking. Now, I would venture a guess that none of us are so criminally minded as to take up hacking other peoples computers to deplete their accounts.

And, I would also surmise that all of us, in varying degrees, are paranoid when it comes to exposing our personal information on-line.

The fear of identity theft may not be sweat inducing but, if you are the victim, it can get the heart racing a bit faster.

First, a few definitions:

Hacking: Computer hacking is broadly defined as intentionally accessing a computer without authorization or exceeds authorized access. Various state and federal laws govern computer hacking.

Hacker - in the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network.

White hat - breaks security for non-malicious reasons.

Black hat - violates computer security for personal gain or just to be malicious.

Gray hat - somewhere between the first two. Hacks for the sole purpose of finding security flaws and then notifying the administrator, sometimes offers to fix the defect for a fee.

Blue hat - someone outside computer security consulting firms who bug-tests system prior to its launch, primarily looking for exploits so they can be closed before going public.

Elite hacker - a social standing among hackers. Used to describe the most skilled hacker.

Script kiddie - unskilled hacker who breaks into systems using automated tools written by others.

Neophyte - 'newbie', or 'noob' someone just starting out in hacking. Limited knowledge or experience.

Bear explained the various types of hackers, from the good to the bad. The 'white hats' are those who may have, at one time, been 'black hats' themselves and now help the authorities to catch and capture the bad guys.

Hackers can be located anywhere in the world. Close proximity is no longer a requisite for stealing your personal property.

Experienced hackers learn a programming language so they can write code to access a target system. Once access is gained, they can write code to have the system execute their bidding.

They then 'ping' a remote system. Ping is a command line entry to find a computer on the internet. A scan of the available ports in the operating system is done to find any that are open. Some ports are well protected while others are open for convenience.

Following their own personal check-off sheet, they incorporate steps as follows:

Use brute force cracking to obtain the password which gives full access.

Then to perpetuate their admission, hackers create a backdoor where they can come and go as they please even though the master password on the system is changed.

CYA -Cover Your Access. Eliminate all traces of your presence, except for the backdoor, so they can't be identified and traced.

Bear then briefly mentioned the **Dark Web**. Here's how StraightDope.com describes it:

"The dark Web is a collection of sites and technologies that don't just hide data but conceal attempts to access it. For example, if I were operating a website for assassins, I'd want not merely to keep my roster of contract killers safe from accidental discovery, I'd also want it to be possible for potential clients to reach me and my site without their efforts being detectable.

(Continued on page 3)

Established 1988

The TUG

MOAA Hawai'i Aloha Chapter Computer User Group

INDEPENDENCE Day

An International Association of Technology & Computer User Groups

Volume 29 Issue 7 www.the-tug.org

Mailing address for The TUG
94-1071 Leomana Place
Waipahu, HI 96797

TUG (The MOAA Hawaii User Group)
by Lou Torraca
http://www.the-tug.org

Cyber Security

Hardly a day goes by without news of another hack of "bazillion" records that contain vital information. Sometimes we receive notification that our information may have been compromised. Pretty scary news to say the least. There are numerous things that can be done if you receive this kind of bad news, but instead of waiting, it's time to be proactive and avoid the problem in the first place!

By following this handy checklist, investing a little time each week and performing a series of simple chores, you can dramatically strengthen your security posture and help you be more secure online, protect valuable, personal information and avoid identity theft.. In addition, your digital life will be more manageable and you will have peace of mind that you are helping protect your family and the extended online community while enjoying the Internet with greater confidence.

Follow this four-week outline and clean up your family's online life with an easy-to-follow timeline and plan:

Week 1: Keep Clean Machines

As a very basic first step, make sure that all web-connected devices - including PCs, mobile phones, Smartphones and tablets - are free from malware and infections. Use this as a launch pad for your month of digital maintenance.

Week 2: Make Sure You're Secure

Building on Week 1, users can enhance the security of their online accounts – a fast and simple way to be safer online. There are quick and easy things you can do that have long-term safety and security benefits.

- **Get two steps ahead:** Turn on two-step authentication
- **Secure your router:** Make sure your router has a strong password and does not broadcast who you are through its name,
- **Make better passwords:** If your passwords are too short or easy to guess, it's like leaving the front door to your home unlocked.
- **Unique account, unique password:** Having separate passwords — at least for key accounts like email, banking,and social networking — helps to thwart cyber criminals.
- **Write it down and keep it safe**: Everyone can forget a password. Keep a list that's ***stored in a safe, secure place*** in your home.
- **Secure your phone:** Use a passcode or a finger swipe to unlock your phone.

Week 3: Digital File Purge and Protection

Tend to your digital records, PCs, phones and any device with storage just as you do for paper files.

- **Clean up your email**
- **File upkeep**
- **Manage subscriptions**
- **Dispose of electronics securely**
- **Update your online photo album**
- **Update your online relationships**
- **Back it up**
- **Empty your trash or recycle bin on all devices**

Week 4: Clean Up Your Online Reputation

Parents and older kids with social media accounts can take an active role in making sure their online

(Continued on page 3)

Mailing address for The TUG
94-1071 Leomana Place
Waipahu, HI 96797

(Continued from page 2)

reputation is squeaky clean.

- **Own your online presence**: Review the privacy and security settings on websites you use to be sure that they remain set to your comfort level for sharing. It's OK to limit with whom you share information.
- **Clean up your social media presence:** Delete old photos and comments that are embarrassing or no longer represent who you are.
- **Update your "online self":** Are your social media sites up to date? Review your personal information and update it where needed.

That's your assignment: be safe out there on the WWW and, if you're careful, you can even have fun J

Aloha, Lou and Pooky

Dark Web(*Continued from page 1*)

That's what the Dark Web lets them do.

Accessing the Dark Web requires special software, special passwords, or both. The worst-kept secret of the Dark Web is Tor, originally an acronym for "The Onion Router." Building on research originally carried out by the U.S. Naval Research Laboratory, the Tor Project became a community effort to design a way for anyone to communicate online without their location or identity being traceable. Most agree the Tor Project was originally created to ensure free expression without fear of government snooping and interference. The reality is when you get a bunch of people together (not all of them notably mature) and give them complete anonymity and freedom from accountability, often it's the worst impulses that dominate, not the best.

Thus on the dark Web you find the doings of the anarchist hacktivists of Anonymous and the folks behind Wikileaks; Islamic jihadist message boards; stolen credit card numbers, for sale singly and by the thousands; drugs of every description; child pornography; prostitute directories; contact info for purported assassins; and mundane wares such as pirated music and movies."

Visit their web site for more on this and other topics.

Some of the methods used by hackers:

Packet analyzer - captures data packets that can be used to capture passwords and other data.

Spoofing/phishing - masquaerading as another website to obtain data/log-in password, etc.

Rootkit - hard to detect method to subvert control of OS.

Social engineering - tactics used to get enough information through intimidation, helpfulness, name dropping, technical scenarios.

RAT's - Remote Access Trojans - A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer.

And, of course, *computer virus*. A self-replicating program that spreads by inserting copies of itself into other executable code or documents.

Keystroke logging - a tool designed to record ("log") every keystroke on an affected machine for later retrieval, usually to allow the user of this tool to gain access to confidential information typed on the affected machine.

As you can see there are any number of ways for a bad guy to infiltrate computers and networks for their own nefarious reasons.

Keeping your anti-virus, firewall and mal-ware software enabled and up to date are your best protection, short of never going on-line.

Mailing address for The TUG
94-1071 Leomana Place
Waipahu, HI 96797

"Too many people are ready to carry the stool when the piano needs to be moved."

Have you noticed the power drain on your mobile device when using the Chrome browser? Well, here's an article that may explain it, with solutions.

http://tinyurl.com/japlgkk

Use an Android phone? Then you should probably read this:

http://tinyurl.com/j695dxf

Apple cider - "Millions of e-book purchasers will get either credits or checks for twice their losses, legal firm Hagens Berman, which helped litigate the class action lawsuit, said on Tuesday. Apple is on the hook for $400 million in damages plus an additional $30 million to pay the legal fees for Hagens Berman and $20 million to the state attorney generals who became involved in the case.

On an individual basis, each plaintiff in the suit will receive $1.57 in credit for most e-books they bought and a $6.93 credit for every e-book purchased that was on the New York Times bestseller list. Consumers who purchased e-books from Amazon, Barnes & Noble, Kobo and Apple between April 1, 2010 and May 21, 2012 are eligible to receive credits deposited directly in their accounts or checks sent through the mail."

Found this on cnet.com. You'll notice the millions the lawyers are going to get. Well, poor me, I get a $13.86 credit on Amazon. That'll get me about a dozen $0.99 books from their library.

"Let's kill all the lawyers," - Henry VI, William Shakespeare.
Of course, I'm just quoting a line from a play and, I am joking.

With the advent of the Space Age we have seen innumerable advantages in technology. Thousands of inventions that have improved the lives of people throughout the world in every conceivable area e.g. Medical, communications, transportation. Many created by collaboration between NASA and private concerns.

Among those inventions are, and one which is not:

- Cordless tools
- Smoke detectors
- Enriched baby food - Formulaid
- Better pacemakers
- TANG. Invented in 1957 by General Foods but found to be well suited for in space use.

Surprisingly, not that many directly related to computer technology. The micro chip had been invented several years before 1961.

Some of the NASA inventions have been adapted for use in computer technology, e.g. miniaturizing components.

Pre-dating the Space Age phenomenon were UFO's.

Unidentified Flying Objects have long been the subject of alien visitors; conspiracies and, of course, government cover-ups.

Did you know, the first recorded North American sighting took place in 1639 - Sixteen Thirty Nine!!

"The first sighting is often credited to the co-founder of Boston, John Winthrop, who did it back in 1639."

There's more on UFO's at - http://triviatoday.com/blog/article.asp

I mention UFO's because I read recently where one of the Presidential candidates has promised to release all the records on Area 51 currently banned from release by the Government. But, then again, Jimmy Carter made a similar promise. As Agent Mulder says, "The truth is out there."

Here's wishing you and yours a safe and happy

Well folks, we've managed to make it through the first 240 years.

I don't want to sound depressing but, at the rate things are going, it's going to be a struggle to make it another 240 years.

Keep the faith and

Happy Birthday, America.

Mailing address for The TUG
94-1071 Leomana Place
Waipahu, HI 96797