



S V E C C

SVECC Newsletter

Sunland Village East Computer Club

November 2011

Volume 8 Issue 11

[Online Safety: Understanding Hackers, Phishers, and Cybercriminals](#)

Inside this issue:

| | |
|-------------------------|----------|
| Online Saftey | 2 |
| Disaster Strikes | 3 |
| Online Saftey | 4 |
| Battery Life | 5 |
| Helpers | 6 |
| Right Click | 7 |
| Exit laughing | 8 |

Monthly Reminders:

- Run Disk Cleanup
- Run CC Cleaner
- Defrag your hard drive
- Manually Update Windows
- Update Malware Bytes
- Run your Anti-virus

Have you ever been the victim of identity theft? Ever been hacked? Here's the first in a series of critical information to help you arm yourself against the surprisingly frightening world of hackers, phishers, and cybercriminals.

Some of our geekier readers will already be familiar with a lot of this material—but maybe you have a grandfather or other relative that could benefit from having this passed on. And if you have your own methods for protecting yourself from hackers and phishers, feel free to share them with other readers in the comments. Otherwise, keep reading—and stay safe.

Why Would Anyone Want to Target Me?

This is a common attitude; it just doesn't occur to most people that a hacker or cybercriminal would think to target them. Because of this, most ordinary users don't even think of security. It sounds

strange and fanciful... like something in a movie! The reality is quite terrifying—most criminals want to target you because they can, and they can probably get away with it. You don't have to have millions (or even thousands) of dollars to be a target. Some cybercriminals will target you because you're vulnerable, and the ones that want your money don't particularly need a lot of it (although some will take every cent if they can manage).

Who Are these Bad Guys?

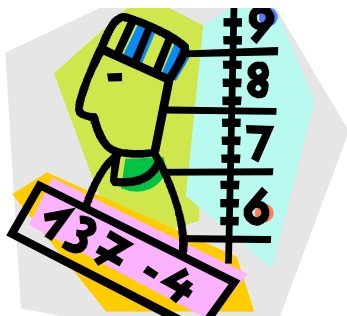
Before we take a look at specifics, it's important to understand who it is that's looking to take advantage of you. Some of the online threats can come from "script kiddies;" hackers with have no real skill, writing viruses using directions found from Google searches, or using downloadable hacker tools for rudimentary results. They're more often

than not teens or college kids, writing malicious code for kicks. While these people can take advantage of you, they're not the biggest threat online. There are career criminals out there looking to rob you—and these are the ones you really have to be aware of.

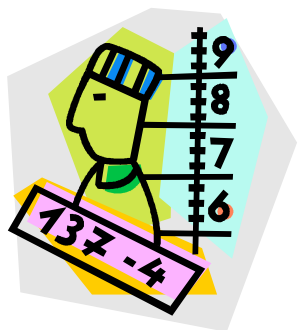
It may sound like hyperbole, but you can quite accurately think of cybercriminals as an internet version of Mafia crime families. Many make their entire living preying on stealing information, credit card numbers, and money from unsuspecting victims. Many are experts, not only at stealing this information, but also from getting caught taking it. Some operations could be small—one or two guys and a few cheap machines for sending phishing emails or spreading keylogging software. Others can be surprisingly large businesses based around [black market sales](#)



[Online Safety: Understanding Hackers, Phishers, and Cybercriminals](#) (Continued from page 1)



If you were skeptical before, hopefully now you're convinced that it's worth your while to protect yourself from the myriad of people hoping to steal from you online.



[of illegally obtained credit card numbers.](#)

What Is A Hacker?

If you were skeptical before, hopefully now you're convinced that it's worth your while to protect yourself from the myriad of people hoping to steal from you online. But that brings us to our next question—just *what is* a hacker? If you've seen any movie since the popularization of the internet... well, you might think you know, but, if you're like most people, you're more wrong than you know. The original meaning of "hacker" applied to the clever computer users, and may have been first coined by MIT engineers like [Richard Stallman](#). These hackers were known for their curiosity and programming skills, testing the limits of the systems of their day. "Hacker" has gradually developed a darker meaning, generally associated with the so-called "[Black Hat](#)" [hackers](#) known for cracking security for profit or stealing sensitive information. "White hat" hackers could crack the same systems, and steal the same data, although

their aims are what make them different. These "white hats" can be thought of as security experts, searching for flaws in security software in order to attempt to improve it, or to simply point out the flaws.

[As most people use the word today,](#)

"hackers" are thieves and criminals. It may not be worth your time to read up on the intricacies of cyberwarfare or the ins and outs of security cracking. Most hackers pose a threat to the everyman by stealing sensitive accounts like email, or those that contain information like credit card or bank account numbers. And *almost all* of that particular kind of account theft comes from cracking or guessing passwords.

Password Strength and Security Cracking: Why You Should Be Afraid

At some point, you should do a search for the [most common account passwords](#) (link contains NSFW language), or read the amazing security article "[How I'd Hack Your Weak Passwords](#)" by John Pozadzides. If you look at cracking

passwords from the hacker perspective, the unwashed masses are basically a sea of vulnerability and ignorance, ripe for the thievery of information. Weak passwords account for the majority of problems ordinary computer users encounter, simply because hackers are going to look for the weakness and attack there—no sense wasting time cracking secure passwords when there are so many that use insecure passwords.

Although there is considerable debate on best practices for passwords, pass phrases, etc, there are some general principals on how to keep yourself safe with secure passwords. Hackers use "[brute force](#)" [programs to crack passwords](#).

These programs simply try one potential password after another until they get the correct one—although there is a catch that makes them more likely to succeed. These programs try common passwords first, and also use dictionary words or names, which are much more common to be included in

When Disaster Strikes Smile

Have you ever deleted photos from a camera or computer by mistake?

A friend of mine called me recently after going through a “catastrophe,” as he called his situation. It happened about midway over the Atlantic Ocean, thirty-seven thousand feet up. He was sitting in his seat with not much to do so he decided to check the photos on his digital camera. All these photos were from this trip to Portugal, a trip that involved hiking in the wilderness and visiting old buildings. You can only imagine some of his prized photos.

I think you know where I am going with this... Yes, while looking at the photos, clicking from one to the next, he inadvertently deleted not just a couple of photos, every photo from his trip was gone in one simple click. After

checking and double checking he knew it was fruitless to look further; the photos vanished.

When he got home he called and told me about this situation.

“That’s no problem,” I tried to reassure him. I explained that there is a software recovery program that people use in such cases with much success. The voice at the other end of the line was silent. I knew he didn’t think this process was possible. After he recovered every single photo from his vacation he couldn’t thank me enough.

However, my tale doesn’t end there. I had a similar problem where a new SD (photo storage card in camera) failed to produce 250 pictures and some video clips. After taking a deep breath I remembered the advice I had doled out and quickly down-

loaded a copy of Recuva, a recovery program that is free and works. Within no time I had all my pictures and video clips stored on my computer, thanks to Recuva.

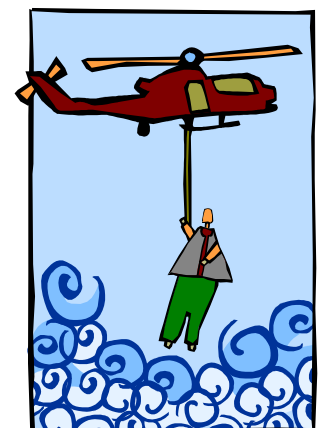
The moral of this story is when you delete photos, music from an MP3 player, or data from your computer, remember that it is possible to recover the data. Don’t say it will never happen because you are careful. I am sure it has happened to the best of us.

To avoid a similar “catastrophe” you need to have a recovery software program installed on your computer. One of the best recovery programs around is called: Recuva. As an added bonus this program is free and it comes “highly” recommended.

You can read the reviews here: <http://cnet.co/filehelp>



The moral of this story is when you delete photos, music from an MP3 player, or data from your computer, remember that it is possible to recover the data.



How to Open Your Favorite Program or Document Automatically at Startup



Use the keyboard shortcut **Windows key + R** to open the Run box. (Hold down both keys.

I frequently advise PC users that they have too many programs running at start up. However, there are also times when you have a favorite program or document or even folder that you want to open whenever you log on. There are several ways to do this but the simplest is to use the Windows system folder named "Startup". Shortcuts to programs, folders, or documents can be placed there. These shortcuts will then be opened

when the user logs on. This is a per-user setting with each user account having its own Startup folder. Here is the procedure.

Quick way to open the Startup folder in all current versions of Windows

1. Use the keyboard shortcut **Windows key + R** to open the Run box. (Hold down both keys.)
2. Type and enter "**shell:startup**" (with out quotes and with

no spaces). Be sure to include the colon.

3. Click "OK". The Startup menu will open.

How to place shortcuts in the Startup folder

Now use the right-click to drag the desired program file, folder, or document into the Startup folder and choose "Create shortcuts here" from the context menu. That's it. Close the Startup folder, log off and then back on and watch your desired objects open.

[Online Safety: Understanding Hackers, Phishers, and Cybercriminals](#) (Continued from page 2)

passwords than random strings of characters.

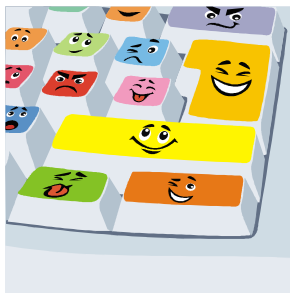
Continued Page 4
And once any one password is cracked, the first thing hackers do is check and see if you *used the same password on any other services.*

If you want to stay safe, the current best practice is to use secure passwords, create unique passwords for

all your accounts, and use a password safe like [KeePass](#) or [LastPass](#). Both are encrypted, password protected safes for complex passwords, and will generate random strings of alphanumeric text nearly impossible to crack by brute force methods.

What's the bottom line here? **Don't** use passwords like "password1234" or

"letmein" or "screen" or "monkey." Your passwords should look more like "stUWajex62ev" in order to keep hackers out of your accounts.



Battery Life

All Lithium-Ion batteries have similar issues. Keep in mind, however, that different chemistries produce very different results, lead acid is very different from NiCd, NiMH, or LiIon. Different batteries using the same general chemistry may still have very different specific chemistry to meet particular cost/current/charge/voltage characteristics. Lithium ion, for example, has at least 8 primary chemistries (e.g. LiPo, LiFe, LiZnCo, etc...), each with a hundred or more variations.

Solar systems often use deep-cycle lead-acid because it is cheap, mature, and very rugged. That makes comparing solar experience to laptops somewhat difficult. Some newer Lithium Ion batteries use new chemistry (e.g. Si cathodes in charge-carrier flexible polymer matrix to accommodate swelling during charge/discharge) to adapt to the issues below, but all still face the same challenges to a greater or lesser extent.

1) Lithium Ion involves actual absorption and release of Lithium atoms by anode and cathode.

This means that there is physical stress on the battery elements, and over time this will damage the materials. Deep discharge cycles and higher current drain will make these happen faster.

Your cell phone battery has low current drain and long cycles, compared to a laptop, and will tend to last longer as a result.

Letting your battery fully discharge before charging

it will cause damage, but LiIon also has an explosive chemistry, so power management circuitry manages the battery, and turns off a phone when there is still about 20% charge left in the cell to mitigate this for cellphone batteries.

The ideal usage is to charge at about 30% and not leave the cell above 70% for too long (see issue 2 for the reason).

2) Lithium Ion current limits are dependent on the Li mobility, which requires highly solvent electrolytes to permit high current usage.

This means that the anode and cathode materials will dissolve in the electrolyte over time, and, because of the electrical potential between anode and cathode, will form whisker structures that eventually short across the gap between the electrodes.

Leaving the cell fully charged for a long time (or constantly charging it when not in use) will encourage these whisker structures to grow because it maintains a higher potential between the electrodes. This is why leaving a battery in a charger for a long time (months or years depending on the battery and charger) will eventually result in a dead battery, even though it was never really used.

Modern charging circuitry could account for this by discharging the battery periodically, but laptops and other consumer-oriented devices generally do not in order to maintain immediate readiness for on-battery use while charging.

The recommendation is to actually use the device powered by the battery from most of the time, and only add A/C power to recharge, when planning to disconnect in the near future, or when usage duration is reasonably expected to exceed battery life (even then starting on battery and adding A/C when charge drops below 50% often helps). It's also best not to leave a laptop always connected to power, and only plug in when charging is actually needed.

In the end, the reason a cell phone battery often lasts so much longer than a laptop battery (typically 2-3 times as many charge/discharge cycles) is more about the different power requirements of the two uses and the specific structure and chemistry choices made to match battery to load. Research is constantly advancing battery and other electrical energy storage technologies, so the performance one may expect for a given usage are constantly changing, and different manufacturers may use very different approaches to meet specific cost and performance criteria. This makes comparing, or even predicting, battery life very difficult, to the point of being little more than a guess, so the best advice I know is to simply use the device in a reasonable manner, and keep an eye on the lifespan indicator via the battery information probe available in Linux so you have some advance warning when you'll need to purchase a new battery.



Solar systems often use deep-cycle lead-acid because it is cheap, mature, and very rugged.





911 Call to help group

What it costs elsewhere

Geek Squad in home call \$149.00 per hour

Serving Online Seniors in home call \$85.00 per hour

On line help \$79.95 subscription + \$24.95 per month

a gratuity to your SVECC helper is recommended

Name _____ Phone _____

Address _____

Brief problem description

Computer Help Group

Group Leader Joe Zagar

| | | |
|-----------|--------------|--------------------------|
| Joe Zagar | 480-373-9373 | all systems and programs |
|-----------|--------------|--------------------------|

Depending on the season we have a number of helpers to assist with problems or installations. Contact Joe Zagar for assistance, referral, or recommendation of local service provider.

In addition on most Thursday's from October to March we offer a fix-it session from 1pm to 3pm at the Training Center. Sessions are open to all residents of SVE and are first come first serve. Charge is \$15.00.

Call ahead to see if your problem can be solved at a Thursday session.

November 2011

| SUN | MON | TUE | WED | THU | FRI | SAT |
|-----|---------------------|--------------------------------|-----|-------------------|-----|-----|
| | | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 Computer Club | 8 SLUG 6 to 9 Patch Tuesday | 9 | 10 ASU Auction | 11 | 12 |
| 13 | 14 Computer Club | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 Computer Club | 22 SLUG 6 to 9 | 23 | 24 | 25 | 26 |
| 27 | 28 Computer Club | 29 | 30 | | | |

I have recently become familiar with some handy uses of the mouse right-click that are worth mentioning.

1. Right click on "Start" brings up a menu that lets you select Microsoft "explorer" and "search." This can be a quick way to get at those utilities.
2. If you want to use a program other than the default in conjunction with a file, then right click on the file and go to "open with." I sometimes use this with pdf files. My default for pdf files is "Nitro" but it does not have a search function, so I will sometimes switch to "Adobe Reader" if I want to use the search.
3. In the tray at the bottom of the screen is an icon that looks like a screen with radiation coming from it. Left click tells the status of your Wi-Fi connection. Right click gives options of disable/status/repair. I was at a location where I appeared to be connected properly, but all of my browsers were unable to reach any URL. Someone assisted me by clicking on "repair" and I could watch the system rework my connection and make it better. I was dazzled.
4. The most important time-saver of all: If you are playing solitaire and you reach the point where you have won the game and it is just a matter of moving all the cards to the top row, then right-click on one of the cards in the bottom row and the system will do the remaining work for you.

SVECC

Check us out at
svecc.com

President
Delores Bruno

Sunland Village East Computer Club

Founded for the Residents of
Sunland Village East

Mission: To help each other learn about Computers

Membership is open to all residents of SVE

Dues are \$20.00 per Year

Due October 1st

Sunland Village East Computer Club



*“Your shoe phone works, but
needs an odor eater.”*

SVECC

Check us out at
svecc.com

People helping
People