GEORGIA STATE DELTA KAPPA GAMMA SISTERS USING TECHNOLOGY IN OUR PROFESSIONAL AND PERSONAL LIVES

Technically Speaking

Georgia Gold
Setting the Gold Standard in DKG

VOLUME II, ISSUE 2 SPRING, 2014

I've Been Hacked! What to Do First?

A few years back, I sat down at my computer to pay some bills. As I coordinated my check register with the online statement, I began to see some unusual charges. Starting with some low amounts ($8.95, $19.99), then becoming higher—and all originating from Spain or other overseas countries. My bank account had been hacked. Of course, my local bank branch was not open, so I had to call their 800 number and begin the process to stop the slow flow of money from my account.

With the recent Target/ Neiman-Marcus security breach, it is estimated that 110 million Americans (or roughly one out of every three people) may have had their information compromised. Our special focus of this edition of Technically Speaking will be online safety—how to keep your information safe, and what to do if your information or bank account has been compromised.

If you still have access to your bank account, immediately change your password. Unfortunately, this is also one of the first thing the hacker will do in order to have unlimited access to your account. If you have other accounts that share the same password, check them also. Immediately contact your bank and notify them of the breach. Most banks have a 24-hour number that you can call. They will immediately cancel your cards. If you notify your bank within two days of the breach, your liability is limited to $50 or the transaction amount if it is less that that. After two days, it can go up to $500. A lot of banks actually catch the first attempts at infiltrating your account as they have security programs that watch for suspicious activity from foreign countries. (If you do plan to travel outside the United States, it's a good idea to call and notify your bank/credit card company so they don't freeze your account when they see these charges coming in!)

Some banks will require you to fill out a police report before they will reimburse your money lost. Unfortunately, there is probably nothing the police can actually do since the people accessing your account are thousands of miles away, but many banks require the police report number for their records. If you have recent bill or store payments, you may need to contact these places and let them know and arrange to pay another way. Since your account is frozen, when these legitimate payments come though and are denied, it can hurt your credit with them.

Continued on page 3

SPECIAL FOCUS: ONLINE SAFETY TIPS

A Publication of Psi State The Delta Kappa Gamma Technology Committee:

Tina Marsh
Allison Dewell
Kathryn Hodges
Miriam McGhee
Anne Peterson
Merry Willis

How to Protect Against Hackers By Allison Dewell

If you send e-mail, post updates on Facebook, check your bank account balance online, or do most anything that requires the Internet, you're at risk of being hacked.

Cybercriminals are experts at tricking people into downloading malicious software that can give them access to your personal information and passwords.

But there are commonsense steps you can take to avoid getting hacked:

1. Be aware of what you share

You don't have to delete your Facebook or Twitter account to say safe, but posting birth dates, graduation years, or your mother's maiden name-info often used to answer security questions to access your accounts online or over the phone-on social-media sites makes a hacker's job even easier.

See page 2 for rest of article.

How to Protect Against Hacking continued...

2. Pick a strong password

It can take a hacker's computer only ten minutes to guess a password made up of six lowercase letters, but free websites such as safepassword.com can help you create a nearly uncrackable password with uppercase letters, symbols, and numbers. Using phrases as passwords works well too (the website passphra.se can help you create them). The phrase "say no to hackers," for instance, would theoretically take a hack thousands of years to guess-until now, that is.

3. Use 2-step verification

Facebook and Gmail have an optional security feature that, once activated, requires you to enter two passwords- your normal password plus a code that the companies text to your phone-to access your account. "The added step is a slight inconvenience that's worth the trouble when the alternative can be getting hacked," says CNET tech writer Matt Elliot. To set up the verification on Gmail, click on Account, then Ssecurity. On Facebook, log in, click on the down icon next to Home, and then click on Account Setting, Security, and finally Login Approvals.

4. Use wi-fi hot spots sparingly

T-Mobile and ATT, the largest providers of free public wireless internet (the kind often available in coffee shops, airports and hotels), don't require encryption of data traveling between laptops and the internet, which means any info-your email pw, your bank account balance-is vulnerable to hackers. In windows, right click on the wireless icon in the taskbar to it off. On a mac, click the wifi icon in the menu bar to turn off wifi.

5. Back up your data

Hackers can delete years' worth of emails, photos, documents and music from your computer in minutes. Protect your digital files by using a simple and free backup system available on websites such as crashplan.com and dropbox.com.

Sources: CNET, Lifehacker, NPR,ABC

Apps to Keep You Safe Online

By Anne Peterson

Everyone knows you need strong passwords to keep your information safe online. The strongest passwords are long and use a combination of upper and lowercase characters, numbers, and punctuation. It's also best to use a different one for each website. That's where it gets complicated. It's hard to keep track of all the passwords you have to use. There are some apps that can make your life easier, and keep your information protected.

Password is the best-known password manager app. Along with a strong password generator, it can also store your personal documents, passport details, addresses and more. In addition, it has a secure browser built into it, allowing you to surf to your bank's website where it will automatically enter your passwords for you. This app excels in security. There's a master password that protects your data, and the data stored inside the app is encrypted with makes it safe even if someone steals your device. It's price tag is high, though, at $18. There is a free Android version, but it's much simpler and you can't enter new data.

LastPass is an alternative password and personal data manager. It stores web site passwords, credit card information and more behind a master password. While the app is free, to make the most of all its powers, you have to pay a subscription of $12 a year.

(continued on page 3)

I'VE BEEN HACKED! WHAT TO DO FIRST?

Continued from Page 1….

What if your identify has been stolen and used to open credit card accounts? You may first realize this when you receive a credit card bill for an account you didn't apply for. Immediately contact the fraud departments of the three largest credit reporting agencies and ask for a report. If you were one of the people who shopped at Target during its breach, they are offering one year of free credit monitoring. The three credit monitoring companies are:

Company	Report Fraud	Other Credit Report	Web Site
Equifax	(800) 525-6285	(800)685-1111	http://www.equifax.com/
Experian	(888)397-3742	(888)397-3742	http://www.experian.com/
Trans Union	(800)680-7289	(800)916-8800	http://www.tuc.com/

Second, contact the creditors for any accounts that have been tampered with or opened fraudulently. Speak with someone in the security or fraud department, and follow up in writing. Following up with a letter is one of the procedures spelled out in the Fair Credit Billing Act for resolving errors on credit billing statements, including charges that you have not made. You also need to file a police report. You may need to send this to creditors to prove that a crime was committed.

Another popular hack is the email account. All of a sudden, your friends begin getting emails saying "Check out this great website…." or "Help! I'm traveling in South America and my wallet was stolen". If the hackers have not yet changed your email password, login and do that immediately. Make it VERY secure—lots of numbers and random letters (NOT your dog's name or important numbers that would be easy to figure out). If your access is blocked, you will need to contact your email provider and recapture your account. The email provider will also have access to tools they have to get you back and running. Next you need to notify everyone on your contact list! Tell them not to open anything from you for a while and to check their computer's protection. Scan your own computer with an anti-viral program. Hackers may not only be interested in your email, but insert a Trojan program (think Trojan horse—it gets in undetected and then attacks) to access your bank and other programs. Change your passwords for all these other accounts, especially if you have used the same password as your email account.

Unfortunately as more of our daily living and communication takes place in cyberspace, the occurrence of hacking is bound in increase. The best way to guard against this happening to you is to monitor your accounts frequently. And if it happens to you, don't panic! There are safeguards in place to help you make it through.

APPS TO KEEP YOU SAFE

..... CONTINUED FROM PAGE 2

OneSafe, on iOS only, is another alternative that stores passwords, credit card data and personal documents. The app is $6 and contains several unique features like pattern lock access, where you swipe a unique pattern on your screen to unlock the data, and an alert if someone tries to swipe your data.

Another app with a strong following of users is **Keeper**. Keeper has many of the same features as the others, but it will allow you to share your data with someone you trust. It is available on Android and iOS.

The iOS $1 **Wolfram Password Generator Reference App** can create strong passwords for you. It comes up with tricky passwords full of letters, numbers, and other characters.

Once you have created strong passwords for your different sites, **iCloud Keychain** can remember them so you don't have to. It stores usernames and passwords and syncs them between your Apple devices.

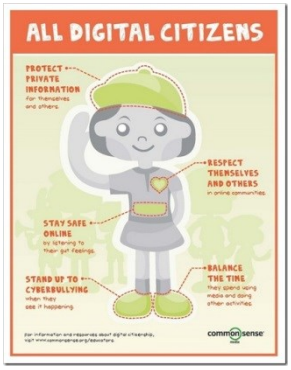
Information source: www.nytimes.com

Teaching Your Children to Be Safe Online

By Kathryn Hodges

Technology is becoming more accessible to students every year. With some schools even allowing students to bring their own devices, it is important to teach students the importance of being safe on the internet. Students should be taught not to talk to strangers on the internet. Having students use a different name is a good idea. Also, make students aware that once they post something on the internet it becomes public. You can't take it back and you shouldn't be mean to others. The following resources will help you teach your students about internet safety. If you use a website or video, take the time to go through it together and discuss it as a group afterwards.

Printable PDFs



http://www.commonsensemedia.org/educators/elementary_poster

http://www.childnet.com/resources

Resources for teaching internet safety:

http://ilearntechnology.com/?p=5127

http://pbskids.org/webonauts/about/

https://learninglab.org/

http://www.covenantworks.com/Bouncy-A/Computer/InternetSafety/index.htm

http://www.brainpopjr.com/artsandtechnology/technology/internetsafety/

PLACES YOU SHOULDN'T USE YOUR DEBIT CARD

By Anne Peterson

Debit cards and credit cards each have their own advantages, one of them being that they're so easy to use. However, with that ease comes some risks with security. Many of us can't imagine life without our debit cards, but if you think about it, using your debit card is really a scary situation. It's a direct line to your bank account and, if hacked, it can be very difficult, if not impossible, to recoup money lost when accessed by hackers.

With that in mind, there are things you can do to prevent your debit card from being hacked. Here are 10 situations where it can pay to leave your debit card in your wallet.

-**Online (including phone orders)**- If you have problems with a purchase, there is no consumer protection, or if the card gets hacked, it can be difficult to get your money back. The Federal Reserve covers debit card transfers, and sets a consumer's liability for fraudulent purchases at $50, provided the bank is notified within two days of discovering the card or card number has been stolen.

-**Purchase of Big-Ticket Items**- Credit cards are safer to use for big-ticket items. Credit cards offer dispute rights if something goes wrong with the merchandise or purchase. Some credit cards even offer extended warranties.

-**When a Deposit is Required**– When you are required to give a security deposit, it's best to use your credit card. That way, the store (or other business) gets their security deposit and you get to keep your cash.

-**Restaurants**- In restaurants, it's especially dangerous to use your debit card. Once the waiter leaves with your card, you have no way of knowing who has access to it, or what is being done with it.

-**Buy Now, Take Delivery Later**– In situations like this, it's best to use a credit card which gives you dispute rights in case of a problem.

-**Recurring Payments**- Besides depending on your own memory and math skills from month-to-month, another reason not to use a debit card for recurring payments is the chance that once you request payments to stop, they could continue to be drafted from your bank account.

-**Future Travel**– If you're making travel plans, book your travel with a credit card or some other means. If you use your debit card, you lose money immediately for a service you may not be utilizing for another six months or more, or at all, if your plans change suddenly.

-**Gas Stations and hotels**– Some gas stations and hotels place holds on your card to cover customers who may leave without settling their bill. In many cases, the hold is placed on your bank account for days, tying up money that you may not have actually spent.

-**Checkouts or ATMs that look "off"**- Take a good look at the machine. If it doesn't fit together well, or something looks as if it doesn't belong on the ATM, leave it alone. Criminals are getting better and better with planting "skimmers" in places you'd never suspect.

Information source: www.creditcards.com