Georgia College

Information Security Training

Presented by the Information Security Office,
updated 9/23/2011

Objective:

Everyone on campus has access to information. As stewards of this information it is imperative that we use and handle the information in a safe, secure, ethical and legal manner. The information in this presentation is designed to provide practical information about information security in today's working environment.

GC Policy:

RESPONSIBILITY FOR ESTABLISHING A SECURE INFORMATION ENVIRONMENT

INTRODUCTION

In order to fulfill its mission of teaching, research, and public service, the University is committed to providing a secure environment that protects the integrity and confidentiality of information while maintaining its accessibility.

PHILOSOPHY

Each member of the GC community shall be responsible for the security and protection of information resources over which he or she utilizes or for which they have responsibility. Resources to be protected are networks, computers, software, data, medical records, financial information, identification information, and personal information. The confidentiality, integrity and availability of these resources must be protected against physical and digital threats including unauthorized intrusion, malicious misuse, inadvertent compromise, force majeure, theft, errors, omissions, or loss of custody and control. Activitie outsourced to corporate or other entities must comply with the same security requirements and meet CIO approval.

GC Policy (continued):

Responsibility for information is controlled by supervisors at the unit level and include:

- Become knowledgeable regarding relevant security requirements and guidelines
- Identify the information resources within areas for which they have responsibility/access
- Establish acceptable levels of risk for resources by assessing factors such as how sensitive the data is (law) or the level of criticality or overall importance to the business continuity of the University
- Ensure compliance with relevant provisions of all federal, state, and local laws
- Become knowledgeable regarding relevant security requirements and guidelines
- Analyze potential threats and evaluate the feasibility of various security measures in order to provide recommendations to the Administrative Officials
- Implement security measures that mitigate threats, consistent with the level of Acceptable risk established by administrative officials
- Establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements

GC Policy (continued):

Users - Individuals who access and use campus electronic information resources must:

- Become knowledgeable about relevant security requirements and guidelines

- Protect the critical resources for which they are responsible, including but not limited to, access passwords, computers, and all information/data in their possession

Information Security:

It's about handling information, not just information on your computer.

It starts with physical security; securing documents, keeping them from prying eyes or from being stolen.

Keep documents face-down on your desk top. Don't allow someone to walk up and discover someone else's private information right there for the observation/taking.

When away from your desk keep files stored in a locked file cabinet and if possible lock the door to your office.

Don't throw documents with sensitive information in the trash can; **shred them**. Identity thieves know too well that the easiest way to find information is through dumpster diving.

Protect media containing sensitive information behind lock and key. CD's, flash drives, etc. should be stored in locked drawers.

Laptops are too easily stolen; keep them locked. Never leave a laptop unattended and unlocked, whether at work, in your car, etc.

What information is considered "sensitive"?

As it ends up, most of the information that we deal with on a day-to-day basis could be considered sensitive and subject to protection. While much of what we deal with is subject to the Open Records Act, that doesn't mean that we want it to make tomorrow's headlines. Additionally there are new laws passed every year geared towards protecting information and personal identities. A few that directly pertain to Georgia College are:

FERPA – protection of student records

HIPAA – protection of people's health & medical records

Red Flag Rule – identity theft protection

GPIPA – personal identity and account number protection

Aside from legislation there's ethical handling of information. If you regard the person's information in front of you as if it were your information and ask yourself "How would I want my information handled?", you'll usually err on the side of security and safety.

Can you be specific?

Certainly there's quite a bit of sensitive information available to most of us. As a rule, try to accomplish the tasks at hand with as little information as possible. For example, if you can look up a student by their name then there's no reason to collect and store their SSN, GCID, etc. Store/Collect as little as possible to get the job done.

The type of information that will get GC in legal trouble would be where we associate a name (doesn't have to be a student) with other information, whether it's ID numbers (GCID, SSN, Credit Card Number, etc.) or class assignment/grades or medical information. If you want to send someone a list of GCID's without any context, that's fine. It's when you link them with names, and in context of "here's a list of everyone who has withdrawn" that we get into trouble.

OK: 911271313
911281439

BAD: 911271313 John Testperson
911281439 M. Testperson
Mary Testperson ACCT 101 A

More specifically:

Many departments need to share lists of students with one another, whether it's a list of students who have withdrawn, or students who've made honor role, students who will be attending our special event, etc. This is required to accomplish the tasks at hand and is a normal part of business operations. However, much of the information that we're passing along is too much information. Keep the information shared/communicated to only the information needed to accomplish the task. Many times we're sending GCID, Name, and then other information. Most departments can look up students by name. If you need to use GCID to make certain you have the correct person, please use only the last 2 or 3 digits:

***121472 Fred Testperson right off this is rather suspicious. It would appear to an untrained eye that we're trying to mask part of their GCID. Not good; 911 prefix is assumed and widely published. For that matter the next 2 digits afterwards are easily guessed. If you simply must use GCID to verify that you have the correct person at hand, mask all but the last 2 or 3 digits, ie. ******472 Fred Testperson will be plenty to tell this person from another with the same name. This same technique could be used for posting grades (as long as they're not posted alphabetically, for example you could post:

******876 97 (where 876 is the last 3 digits of their GCID and 97 is their grade)
******471 100
******655 85

FERPA:

Family **E**ducational **R**ights and **P**rivacy **A**ct: passed by Congress in 1974 and applies to all educational agencies or institutions that receive federal funds administered by the Department of Education. Its provisions apply to all students enrolled at a college or university, regardless of age.

- Access only the records you need to effectively complete your job responsibilities.
- Don't release a students information to ANYONE other than the student or school official (with a legitimate education interest, such as an advisor, dean, registrar, etc.). You must have written consent from the student before you can release information to the parent.
- Do not provide class rosters to anyone. Do not release student email or mailing addresses. Do not assist anyone (other than a University employee) finding a student.
- Do not share information such as grades by email or phone unless you can confirm that the person to whom you are speaking is your student.
- Do not circulate printed class lists with GCID's or grades as an attendance roster. Don't publicly post grades with names or GCID's (you may use the last 3 digits of the GCID if the class roster is not sorted alphabetically).
- Don't leave graded tests or papers in a stack for students to pick up by sorting through the papers of other students (this is considered the same as publically posting grades).

Technology:

While much of the information that we use daily is printed, most of it is used/accessed/seen electronically when we use our computers. As custodians and stewards of this information we need to take the same care of these files as we do the physical printed information.

Acquire and store only the information that you need to accomplish the job at hand. If you have to store the information (file) for any duration of time, it's best to store the file on a campus drive vs. the drive on your PC. This way if your PC were lost or stolen the data remains on campus and not with the PC. Also if your computer crashes with a total hard drive failure, the data isn't lost because it's stored elsewhere. For access to a network/share drive, please contact the Serve Help Desk at x7378. They call it a "Q drive".

If you simply must store the information on your hard drive, know that the password to the computer IS NOT securing the information/data. All a criminal has to do is to remove the hard drive and attach it as a secondary drive to another computer and immediately they have access to ALL of the information stored on that disk. Sensitive files on PC's should be encrypted. Encryption prevents the file from being used/read by anyone other than the person who has the password.

Encryption:

There are two main types of file encryption that we encourage at GC; the use of file or folder (directory) encryption using AxCrypt and full hard drive encryption using TrueCrypt.

Full hard drive encryption literally encrypts everything on the hard drive. When a person wants to boot the PC, the first prompt (before the boot sequence can be initiated) is for the encryption password. If successful the boot sequence continues, and if not it's halted. Not only is the PC prevented from being booted, if it's stolen it prevents the criminal from obtaining the information on the disk by removing it as we talked about earlier. This feature makes this type of encryption ideal for laptops that are mobile and far more likely to be lost or stolen.

File encryption should be used any time you store files on your computer that contain the sensitive information described earlier. AxCrypt should be on your PC already. Make certain that you following GC Policy when creating the password, and be 100% certain that you can remember the password. Once encrypted, if you forget the password, there is no administrator over-ride/recovery.

GC Password Policy: www2.gcsu.edu/policies/overall/password-policy.htm

Your computer:

Good secure practices begin with maintaining the good health of your computer. When initially installed your PC is up to date with operating system patches, virus software, and malware prevention software. It is up to you to make certain that these are all kept current and active.

Screen savers are not only healthy for the hardware, they can be used to secure your PC when you're away by having the screen saver password protected. Use these so that it requires your GC domain password to get back to your PC. Choose low settings (ala. 5 minutes or less) so that when you walk away from your PC unexpectedly the screen is quickly covered by the screen saver. If you're dealing with sensitive information regularly where people can easily look over your shoulder you should purchase a privacy screen for your PC.

Using your computer effectively and securely:

There are two main sections to data handling; storage and transmission.

Storage:

Most of us on campus have access to files that contain sensitive information. If these are managed through software (like Banner, or Paws) the systems take care of the storage for us by keeping the data in a centralized system that is secured. However, many files that we'll use aren't stored in central repositories and are collected and managed by individuals and departments. Whenever possible these files should not be stored on individual PC's. Rather, set up additional network drives that can be shared amongst departmental members as needed. This way the data doesn't reside on the PC. If the PC is lost or stolen or crashes the data isn't compromised or lost. To get one set up, contact the Serve Help Desk and ask about a "Q Drive".

When files are not being used they should be considered candidates for encrypting.

Data transmission:

Our PC's are networked. We attach to the network using either a wire or using a "wireless" signal. Whether you're just logging in on your PC (using your GC domain credentials), or accessing Paws, or going to the internet to read email, etc. all communications to/from all PC's uses TCP/IP. Without getting into too much detail, TCP/IP is a broadcast protocol that transmits data across the network. At the low level each packet of information has an address for the recipient. However, this IS NOT a point-to-point private communication. It's a broadcast (much like a radio signal) that anyone with a very simple packet sniffer can read all unencrypted network traffic. Any unencrypted data transmission can be seen by anyone. Whether email, or chat sessions, if it's not encrypted it IS readable by anyone.

HTTP vs. HTTPS: Most of our network use is through browsers using URL's which begin with HTTP (HyperText Transfer Protocol). HTTP (without the S) is unsecured and visible to prying eyes and susceptible to different attacks without you (the user) ever knowing. The important one is HTTPS, where the S stands for Secure (using SSL; Secure Sockets Layer), which is ENCRYPTED. This constitutes a private point-to-point conversation between your PC and the server that you are accessing.

Data transmission (continued):

Whether going across to the internet or using the intranet here on campus, any sensitive information transmitted needs to be done using an encrypted channel. If you use PAWS or Banner you'll notice the URL's have HTTPS (https://...) enabled. They're encrypted.

Many of us on campus have access to systems outside of Georgia College's control and must use these systems for campus business. For example the athletics department regularly sends and receives information from the NCAA. Some departments have access to and use credit card systems. Any time you're accessing a system, whether internal to GC (like PAWS or Banner) or external, please verify that the URL used shows HTTPS so that the session is encrypted. Otherwise assume that anyone can see your communication and you are probably violating a law.

Email:

Over the past 15 years email and texting have surpassed the telephone to become the de facto standard for communications. As a result, email is now the single most critical system to all campus operations.

Standard/default email is NOT encrypted. While you may notice that the URL for our new live.com email system is encrypted, that encrypted session is only between your PC and MicroSoft while you are logged in. Emails can be forwarded to other systems and these are usually not encrypted sessions (either in the sending/forwarding of the email or in the viewing of the email). For this reason (and others, as email is NOT a guaranteed delivery system) **never send sensitive data or information through email that is *unencrypted*.** Do NOT put sensitive information in the body of an email. Sensitive information should be in a file, and that file should be encrypted.

Email is a very powerful tool. You CAN use it to send an encrypted file. However, make certain to never share the encryption password through email. That would be like locking the front door to your house and taping your key to the outside of the door with a big note saying you'll be away from the house for a week.

Email (continued):

Email is NOT an authenticated system. Just because an email comes in from account.verification@bofa.com doesn't mean that Bank of America sent it at all. It's very easy to spoof an email sender's address. This is by design. We use this technique at Georgia College to send out emails to students for surveys that appear to be sent from the department chair, when in reality the email was sent from a GC server programmatically. We do this so that if someone wants to reply to the email there's a person on the other end. This same technique is used daily by criminals with malicious intent so as to disguise or hide who actually sent the message.

This doesn't mean that your account to email doesn't have authentication; it does. You've been authenticated to have a "live.com" and you have a password to your @gcsu.edu account. Guard it closely! However, just because you received an email from someone that does not guarantee that they're who actually sent it to you.

With all of this open communication that most anyone can see, and knowing that email isn't an authenticated system, how can you trust it? That's a good question. Most email did come from the sender shown. When you receive unsolicited email, especially if it evokes emotion [like you're getting audited], ask yourself if this seems normal. Ask if you expected an email from that person or entity. If the answer is No, then don't respond to it.

Don't be a victim:

Cyber crime is rampant. Criminals WANT your information. Stalkers constantly seek details about you like your age, address, etc. From the small time hacker to organized crime, new schemes come out every day to gain access to your bank account and credit card or worse. Some steal your very identity and open new credit cards under your name and put you in financial crisis for years.

GUARD YOUR INFORMATION. Do not provide your information to anyone that you do not know. Never give this information to anyone over the phone unless you initiate the phone call (ie. how do you know they are who they claim to be).

Thieves are clever. They use clever tactics to disguise their true identity and their true motive. They can be aggressive without you even recognizing it. It's becoming common now for them to scare you right off into making a hasty reaction as a defense mechanism only to get you to reveal your personal information. For example it's common for the phone call or the email to come in saying "We've detected some unusual activity on your account and we'd like your approval to acknowledge the $1,455.32 charge to your account at Larry's Lizard Hut in Phoenix, Arizona. May I please verify that you are Mary Smith at 101 Main Street? For our verification, would you please tell me your account number." And that's how it begins.

Don't be a victim (continued):

The act of trying to get you to reveal information has been called phishing. Phishing via. phone calls has been going on for many years. Thieves use information about you that is easily accessible (like in a phone book) to gain your confidence and suddenly you're revealing your private information. As email became more prevalent as a communications method phishing moved online. It's VERY easy for an official looking email to be constructed using the actual images from legitimate businesses. Below are a few examples of phishes out today:

Bank of America

At Bank of America we appreciate our customers. As a loyal customer you have been approved to receive an interest free loan for $10,000 for up to 3 years. Click here to receive details of this promotion: **I WANT MY INTEREST FREE LOAN**

Don't be a victim (continued):

NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

Defending Our Nation. Securing The Future.

Dear users,

A **important vulnerability** has been discovered in a certain types of our token devices. Please, check that **your token device is safe,** checking the following **link.** If your token is listed as unsafe, please, **download and install** the maintenance update, available **here.** It will exclude the possibility of abuse.

Don't be a victim (continued):

IRS.gov

This is official notice from the Internal Revenue Service that you are being audited for unreported income on your 2009 income tax return for a total of $ 17,381.22 including taxes and penalties.

To avoid additional penalties please remit a check at this time to:
Department of the Treasury
Internal Revenue Service Center
Cincinnati, OH 45999-007

To dispute this claim please go to the **IRS Service Center** website and fill in details regarding your dispute.

Don't be a victim (continued):

Here are a few other examples of images that may show up associated with phishing expeditions and how easy it is to obtain and use official images for criminal activities. These are just EXAMPLES and are not meant to imply that these companies engage in phishing. Also phishing is not limited to only these. Thieves are clever and are getting more sophisticated every day.

SunTrust

VISA

Wachovia
A Wells Fargo Company

MidSouth Community FCU
75
1936-2011
years

WELLS FARGO

Together we'll go far

Don't be a victim -> PHISHING

We've seen a few examples of phishing emails that are circulating at this time. The criminals aim to scare or entice you to supply all types of information, from your SSN and Name (like in the IRS example) to your user ID and password or your bank account / credit card information. They'll use scare tactics that make you think someone has stolen your credit card and made charges on it, or they'll say your back account is overdrawn, etc.

At least once a year someone on campus will fall for a GC phish (appears to be from GC but isn't) scaring them into supplying their GC email account and password. Thieves use these compromised accounts to send spam. While this may seem harmless, the result is that GC will get "blacklisted" and email coming from our campus will be denied by other email servers so that our email system will end up isolated and cut-off from the outside world. It takes many days and quite a bit of effort to get "gcsu.edu" off of blacklists once listed.

By simply clicking on a link from that email you may unknowingly download a virus or malware. Keep your virus protection software loaded and up to date, and the same for malware protection (we use Malwarebytes).

Please know that no legitimate business, university, etc. will ever send you this type of email where they're asking you for your personal information.

The Internet:

The internet is an amazing resource and the volume of information stored/shared grows exponentially every year. With that growth comes risk; new risk every day. Know that criminals are out there and they're looking and scheming. Don't make yourself a target.

Social networking sites are the latest craze and are wonderful for catching up with long lost friends and can help facilitate making new friends. BE CAREFUL. Too much information is just that; too much. Under no circumstance should you ever post your phone number, address, etc. While it's very vogue at this time, it's a bad idea to post your actual date of birth on these sites. Your date of birth is one of the key "secrets" to stealing your identity. Also, social networking sites are by far the largest servers of viruses and malware. Their systems are generally clean, but the links that you click outside their systems (ala. the video's posted, etc.) are highly likely to distribute malicious software without your knowledge. Be suspicious. If you weren't expecting something from that specific person, don't click on links or load video's, etc.

Don't post photo's that are incriminating or show yourself in a negative light. Employers check these, as do police departments. If you're seen in many pictures with a red cup in your hand, while these pictures might not be offensive if you're trying to get a job with a beer distributor, they may not be seen in the same light by other potential employers.

Hosted Applications and "the cloud":

It's very popular today to use hosted applications rather than purchasing hardware and software and having to spend money maintaining a system. Often times, to do this adequately, we're having to move campus data to vendor hosted systems. Or, as in "the cloud", we're just moving campus information there for ease of storage and sharing. These can all make perfect business sense. However, please be careful before entering into any agreement and understand campus liability should information be lost or compromised.

If compromised:

Under most federal regulations and GPIPA, in order to mitigate further damage the University is required to enroll (at University expense) an each person in an identity theft prevention and monitoring program. These usually cost the University between $250 to $500 per account, the average lately has been in the $400 range (per person who've had their information lost, stolen, or compromised). If you were to have only currently enrolled student records compromised, the University would be liable to the tune of a minimum of $1.6M, but really more in the range of $2.6M. If you were to lose just 1 class enrollment file (that wasn't encrypted), that 40 student record loss would cost the campus roughly $16,000 as mandated by federal and state law.

Hosted Applications and "the cloud" (continued):

When entering into contracts with vendors who will be housing GC data, please make certain there's an assignment of liability (to the vendor) and that the limit isn't set too low. A good contract will also have a sunset clause where upon contract termination the vendor will remove or destroy all GC information from their systems.

Question: When accessing these systems via. a browser, what should the URL begin with?

Answer: Hopefully you thought of HTTPS (https://.....); **encryption!**

The same goes for "the cloud". It's unlikely that we'll have a contract with a cloud computing vendor/solution, so there is no assignment of liability. You and the campus retain all liability. And remember, all communication is going over TCP/IP, which without encryption is "in the clear". KEEP IT ENCRYPTED. If you can, encrypt files before storing them in the cloud. That way they're just that much more secure. Remember: how would you want your information handled?

Best Practices:

PCs should be kept in secure places where they cannot be easily stolen.

Keep/store only data required to accomplish a business objective.

Laptops should use hard-drive encryption so that if they are lost or stolen any data on them cannot be compromised.

File cabinets should be kept locked with limited access to the keys.

Sensitive data that needs to be transmitted should be encrypted before sending, so that only the authorized recipient of the data can decipher the information. For a tutorial, see: http://www.gcsu.edu/technology/docs/How_To_Encrypt.pdf

Passwords; use them! Don't use passwords that are guessable. Follow GC standards by making them at least 8 characters long (12+ preferable) and a mixture of upper case, lower case, and at least one special character and one numeric character.

Look for https:// in URL's. Don't supply sensitive information unless the session is encrypted.

Don't:

Do not leave papers on the top of your desk that have personal identifiable information on them (or test grades, etc.) where a passerby could easily obtain the information.

Do not leave file cabinets unlocked when going to lunch or going home for the evening.

Do not send files through email that aren't encrypted.

Do not send personal identification information as part of the body of an email.

Do not post (for public view) personal identifiable information.

Do not send any passwords, user accounts, etc. to anyone through email. GC will never ask you to do so. Do not share passwords with anyone.

Do not use GCID in public, not even posting of grades. Do not circulate a printed class list with GCID numbers or grades as an attendance roster.

Do not release student addresses or email addresses. Do not release class rosters.