Cambridge College

Data Security

Cambridge College
IT Department

Topics

- Overview: Data Security
- Legal standards for data security
- What are we protecting?
- What threats exist and where they come from
- Current policies to protect us
- How to recognize threats and secure yourself from them
- How to respond to threats individually
- How Cambridge College responds
  - What happens after a breach?
- Helpful tips

What is Data Security?

Data security means protecting data, such as a database stored electronically or data contained in paper files, from destructive forces and the unwanted actions of unauthorized users.

Data Security Standards

- Information Security Laws and Regulations include, but are not limited to:
  - Family Educational Rights and Privacy Act (FERPA)
  - Payment Card Industry Data Security Standard (PCIDSS)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - MA Personally Identifiable Information – 201 CMR 17.00: Standards for the Protection of Personal Information

What Data does Cambridge College have to protect?

- Data is gathered on a daily basis for a number of reasons, financial information, research, education, etc.
- Not all information collected is sensitive data
- Cambridge College is obligated to secure sensitive data, specifically:
  - **Protected Health Information**
  - **Student Records**
  - **Personally Identifiable Data**
    - **According to the state of Massachusetts, personally identifiable data is: First Name and Last Name *and* any of the following pieces of information: Social Security Number, home address, drivers license number, date of birth, passport number, bank account information, credit or debit card numbers, copies of birth certificates**

Is it Personally Identifiable Information?

Your middle name	No
Date of Birth	If paired with other info
Passport Number	Yes
Favorite Color	No
Account Passwords	If paired with other info

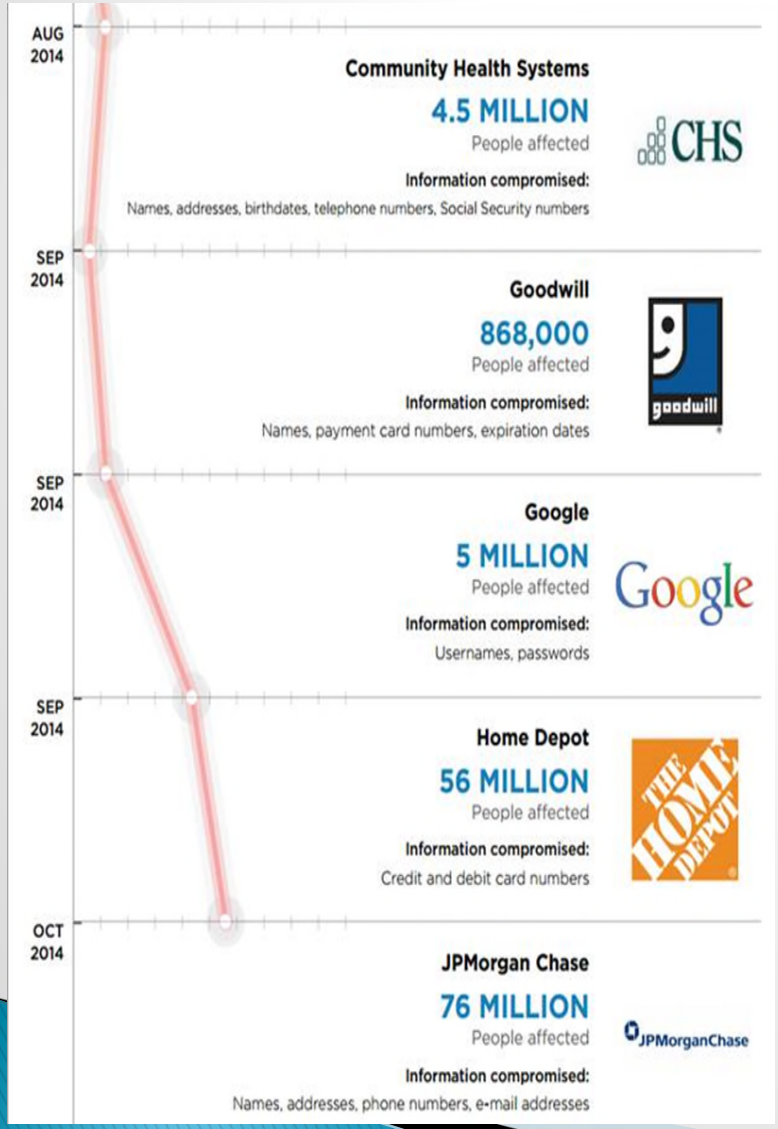
FERPA Defined Directory Information

Directory information at Cambridge College includes name, class year, home address and telephone number, e-mail address, dates of attendance, program status/major, degrees awarded, high school and any college previously attended.

Why should you worry about Data Security?

- We could be penalized as an institution
- Departments could be penalized per incident
- Criminal prosecution for the individual

Recent Data Breaches



Data breaches are extremely costly to organizations, both in repayment of individuals whose information has been compromised and legal fines.

Some Universities have their websites hacked for various reasons. This causes disruptions in workflow, productivity and creates frustrations for students as well as employees.

Mass. Maritime website is hacked

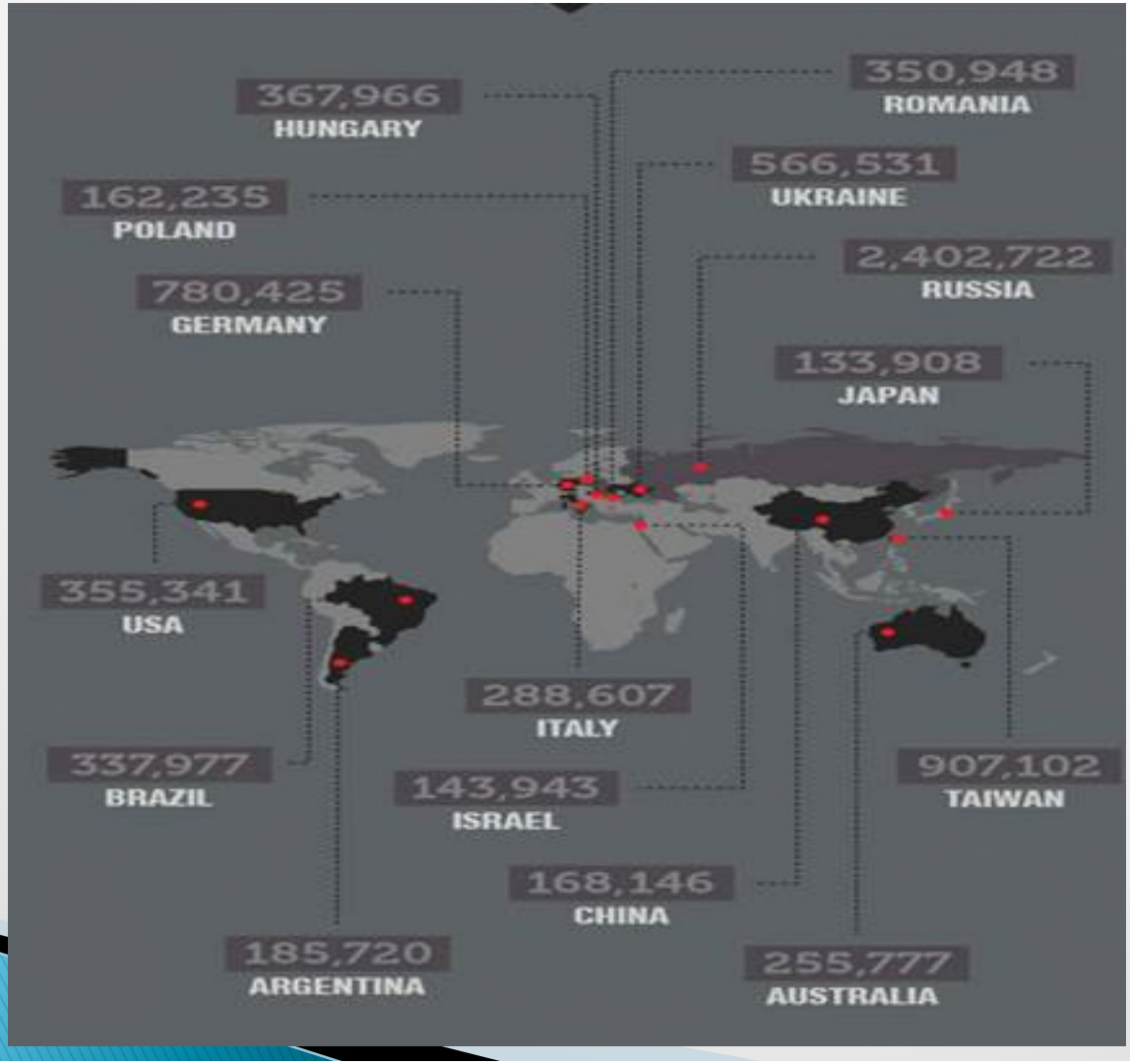
By Trisha Thadani | GLOBE CORRESPONDENT OCTOBER 07, 2014

1 COMMENT

The Massachusetts Maritime Academy's website was hacked Monday in what appeared to be a cyber-attack by an Islamic extremist group, officials said.

Data Security

Where do the threats we face originate?



Source: www.voicetrust.com

Data Security

What targets are being hit?

Industry	% of Attacks
Medical, Healthcare	38.9%
Business	35.1%
Educational	10.7%
Banking, Credit, Financial	5.3%
Government, Military	9.9%

Source: www.voicetrust.com

Data Security

What types of threats should we be prepared for?

Methods of Attack
Viruses, Malware, Worms, Trojans
Criminal Insider
Device Theft
SQL injection
Phishing
Web-based attacks
Social Engineering
Other

Source: http://www.insecpro.com

How do we Protect Ourselves?

College Policies

- Data Security Policy
- Electronic Communication Policy
- Remote Access Policy
- Responsible Use Policy
- Wireless Network Policy

- Details on Cambridge College group policies can be found on the website under the Legal heading at the bottom of each page or the MyCC Portal under the Resources Tab.

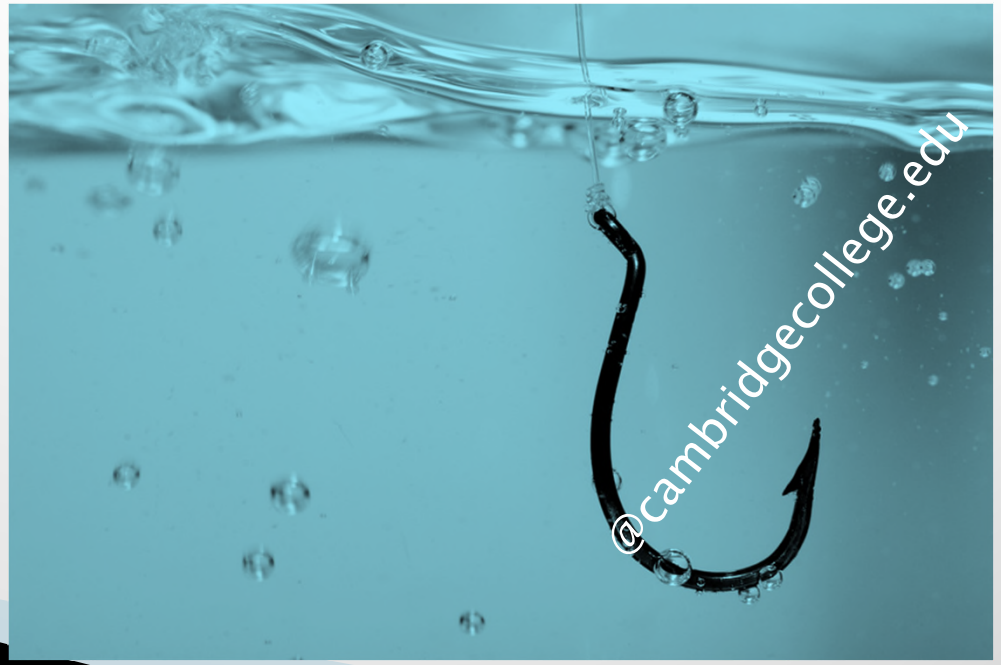
Data Security at Cambridge College

Infrastructure Protections in Place:

- Firewalls
- Symantec
- E-mail protection
- Password protected devices
- Wireless protection
- Group policies for Cambridge College issued machines

E-mail Security

- Microsoft and Google administer spam filters
- If you suspect you received a Phishing e-mail, do not respond to the e-mail at all. Notify the IT Department of the suspicious e-mail immediately by calling the Help Desk



Is it a legitimate e-mail?

From: [redacted] [mailto:michaelrobert56920@gmail.com]
Sent: Tuesday, August 26, 2014 5:27 PM
To: [redacted]
Subject: Sad News!

Hi,

I am sorry for reaching you rather too late due to the situation of things right now. My family and I made an unannounced trip to (Indonesia) for a programme. The programme was successful, but our journey has turned sour. everything was going fine until last night when we were mugged in an alley by a gang of thugs on our way back from shopping. All cash,credit cards and phones were stolen away including some valuable items, It was a terrible experience but the good thing is that they didn't hurt anyone or made away with our passports. I've report to the local authorities and canceled all our cards.

I'm really having some difficulties clearing our hotel bills..We're financially strapped due to the unexpected robbery attack. I'll be indeed grateful if i can get a loan of $2,750 from you. This will enable me sort our hotel bills. but anything you can spare pending when we get things straightened out will be appreciated and I promise to refund it back as soon as we arrive home safely. Let me know what you can do so I can tell you how to get the money to me.

Kind regards

[redacted]

<~WRD000.jpg> This email is free from viruses and malware because avast! Antivirus protection is active.

Is it a legitimate e-mail?

From: HelpDesk
Sent: Wednesday, October 15, 2014 10:59 AM
To: Hunt, Angie
Subject: Your request has been logged with request id ##23969##

Thank you for your ticket inquiry.

Please Note

The HelpDesk does not accept inbound messages. We do this to eliminate spam, and better serve you.

A technician will contact you with a solution through the eHelpDesk's messaging system. ***To respond, follow the link below in the e-mail to update this ticket.***

https://helpdesk.cambridgecollege.edu/WorkOrder.do?woMode=viewWO&woID=23969

If you do not receive a response from the eHelpDesk in 24 hours, a technician will contact you directly using the phone or e-mail information you provided when entering your ticket.

Thank you for using the eHelpDesk,
Information Technology Department
Cambridge College

IT eHelpDesk
617.873.0159

Cambridge College Responses to Phishing Attempts

Dear Cambridge College Community,

Recently, an email was sent to members of the Cambridge College Community titled "Notice from ITS Service Information" stating that "You are currently running on low mail Quota due to hidden files and folder on your mailbox." The email asked you to "Please Click Here to validate/confirm your account", and is from the "ITS Admin at rentonschools.us ".

You should not click on the link. If you received this phishing email please delete it immediately. You do not need to contact the IT department with a confirmation.

Just a reminder from previous phishing incidents:

The IT department will never ask you for your email password in this fashion. Do not ever give your password out to anyone.
If a member of the IT department is working with you directly they may require your assistance and account credentials in order to troubleshoot your account. If this occurs the IT technician will reset your password afterwards and require that you change it again after the troubleshooting session is completed.

As always, we appreciate your consideration of the time dedicated to these phishing and SPAM attempts. We continue to ask for you continued compliance with stated policies so that these incidents never propagate beyond deleting these obvious malware/phishing/virus attempts.

If you have any further questions, or you have responded to the false solicitation, please do not hesitate to contact the eHelpdesk at 617-873-0159 or 1-800-877-4723 ext. 1159.

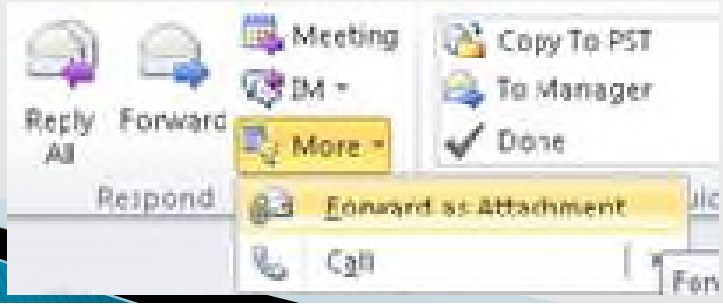
Recognizing Spam & Phishing Attempts

Often phishing scams will contain:

1. Alarming messages or threats of account closures,
2. Promises of money for little or no effort,
3. Requests to donate to a charity,
4. Bad grammar and misspellings
5. Links in the email to unknown sites

If you suspect an e-mail may be a Phishing attempt, please place an eHelpDesk ticket ASAP.

If you receive spam or junk e-mail, you can forward it to junk@office365.microsoft.com, and make sure to forward it as an attachment.



Cambridge College Responses to Security Threats

Cambridge College
Information Technology Department
Phone: 800-877-4723 Ext.1159
Website: http://www.cambridgecollege.edu/information-technology

Dear Cambridge College Community:

As you may have heard, the recently publicized Heartbleed bug in OpenSSL has affected multiple systems throughout the web. This security hole makes it possible for your private communications to be viewed and used by unwanted persons over the Internet. The Cambridge College IT department has already installed software patches issued by our various providers, to all of our systems to ensure the security of our network.

You can learn more about it at www.heartbleed.com. In light of this issue, you may choose to change all of your online passwords as a personal security measure.

Please remember, the Cambridge College IT Department will never ever ask you for your Password. Do not ever provide your password to anyone.

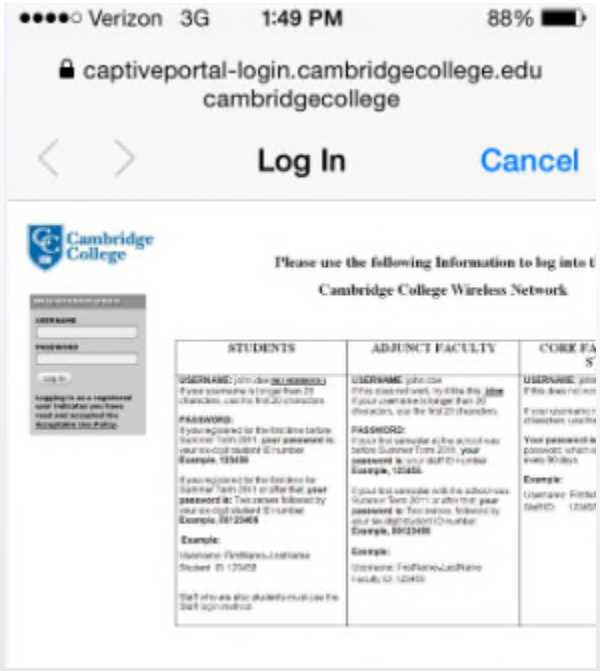
As always, if you have any questions or need technical assistance please place a request through the eHelpdesk system at https://helpdesk.cambridgecollege.edu or call our Helpdesk at 617-873-0159, or toll free at 1-800-877-4723 x1159.

Thank you for your cooperation,

The Cambridge College IT Department

Endpoint and Wireless Security

- Cambridge College provides wireless networking services in public spaces on each campus to enable the convenience of mobile network connectivity. This service allows members of the College community to access the campus wide network from wireless devices or portable computers where coverage is available.



Who is Responsible for Data?

Administrative Area	Data Custodian
Alumni and Development Data	VP for Advancement
Financial Data	College Controller
Financial Aid Data	Director of Financial Aid
Human Resources Data	Director of Human Resources
Information Technology Data	Director of Information Technology
Student Services Data	VP of Enrollment Management

From the Cambridge College Data Security Policy, accessible through MyCC under the resources tab

Data Guardians

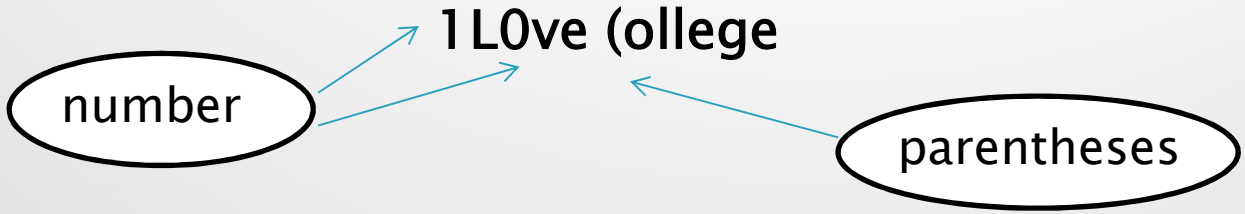
- Data Security is *your* responsibility
- Each employee is a data guardian
- A data guardian is defined as anyone who, as a function of their position at Cambridge College, possesses or has access to Cambridge College administrative data, either electronic or otherwise.

How to Keep Your Data Secure

- Choose a strong password that cannot be easily guessed
- Never give out your password (the Cambridge College IT Department will never ask you for your password)
- Don't keep your password out in the open on your desk (ie: Not on post-it notes)
- Use dynamic passwords

  Example:

  1. Think of a phrase : "**I Love College**"
  2. Make it into a password without spaces: **ILoveCollege**
  3. Add dynamic attributes:



How to Keep Your Data Secure

- Lock your screen or device when you leave your desk
- Be careful of what sites you visit, and what you download to your computer
- Be wary of unsolicited communications from outside sources or asks for personal information
- Do not plug personal devices into your Cambridge College computer (i.e. cellphones, USB drives)

Password Security

- The Cambridge College IT Department recommends a **strong password that contains at least one uppercase, one lowercase letter along with at least one number and one special character (such as: ! # $). The password must be at least 8 characters in length.**

- Cambridge College requires passwords to be changed every 90 days

Reporting Security Related Incidents

Who to contact?

- Contact the IT Helpdesk by placing an eHelpdesk ticket or calling the IT Department directly at (617) 873-0159. Also contact the Director of IT if you suspected sensitive data has been breach. Immediate notification requirements may apply.
- If your Cambridge College issued laptop is stolen, report it immediately to the Cambridge College IT Department.
- If your hardware is stolen from Cambridge College property, notify the Cambridge College IT Department as well as Facilities so they may file a report.

10 Helpful Tips for IT Security

1.) Don’t get tricked
2.) Stay secure
3.) Put things away
4.) Lock it
5.) Stay alert
6.) Protect it
7.) Strong Passwords
8.) Read before you click
9.) Don’t plug it in
10.) Don’t install it

Security Threats Evolving

- Please keep in mind that new ways of trying to illicitly obtain data or present other threats to network security are being created every day.

  Reach out to the IT Department if you have a question or concern regarding network or other data security issues.

  Phone: 617-873-0174
- Email: HelpDesk@cambridgecollege.edu

Helpful Resources

- Cambridge College Policies on MyCC
- http://www.staysafeonline.org/
- https://www.ftccomplaintassistant.gov
- FERPA – http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html