



CARTHAGE
COLLEGE

Security Awareness Part II IT Security at Carthage

July 2017

Session I covered basic IT Security Awareness Training

Today's session will cover:

- How these security concepts apply to Carthage
- Introduction to the new IT Security & Acceptable Use of Technology Policy

Objective: Provide tools and resources for all members of the College community to take responsibility for IT Security



Session 1 Recap

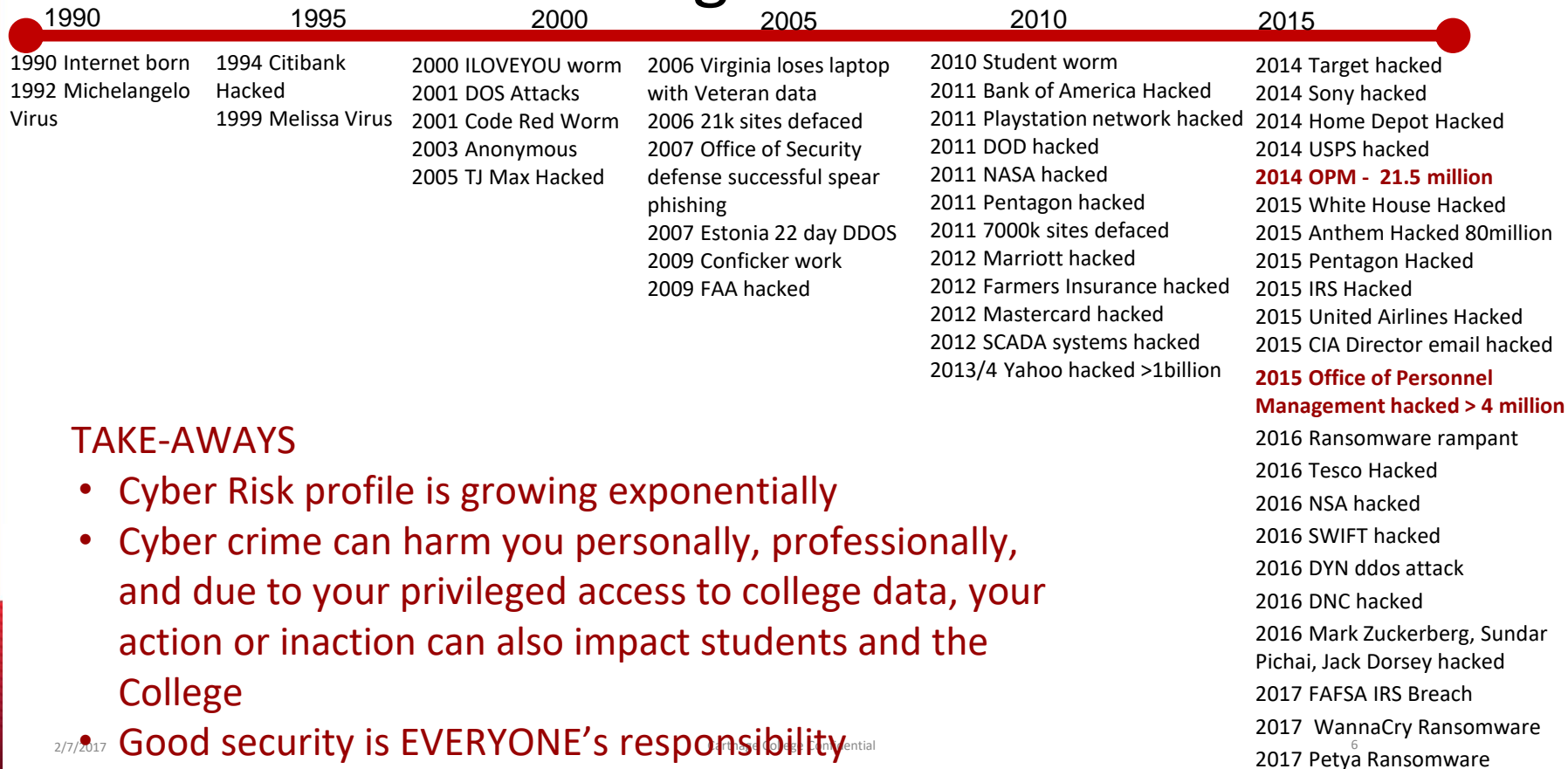
Reminded you to beware of Phishing Campaigns
Beware of Public WiFi
Follow good password practices
Use Multi-Factor Authentication when available
Secure your Devices



Increasing Threat Profile

1990	1995	2000	2005	2010	2015
1990 Internet born	1994 Citibank Hacked	2000 ILOVEYOU worm	2006 Virginia loses laptop with Veteran data	2010 Student worm	2014 Target hacked
1992 Michelangelo Virus	1999 Melissa Virus	2001 DOS Attacks	2006 21k sites defaced	2011 Bank of America Hacked	2014 Sony hacked
		2001 Code Red Worm	2007 Office of Security defense successful spear phishing	2011 Playstation network hacked	2014 Home Depot Hacked
		2003 Anonymous	2007 Estonia 22 day DDOS	2011 DOD hacked	2014 USPS hacked
		2004 Blaster Worm	2009 Conficker work	2011 NASA hacked	2014 OPM - 21.5 million
		2005 TJ Max Hacked	2009 FAA hacked	2011 Pentagon hacked	2015 White House Hacked
				2011 7000k sites defaced	2015 Anthem Hacked 80million
				2012 Marriott hacked	2015 Pentagon Hacked
				2012 Farmers Insurance hacked	2015 IRS Hacked
				2012 Mastercard hacked	2015 United Airlines Hacked
				2012 SCADA systems hacked	2015 CIA Director email hacked
				2013/4 Yahoo hacked >1billion	2015 Office of Personnel Management hacked > 4 million
					2016 Ransomware rampant
					2016 Tesco Hacked
					2016 NSA hacked
					2016 SWIFT hacked
					2016 DYN ddos attack
					2016 DNC hacked
					2016 Mark Zuckerberg, Sundar Pichai, Jack Dorsey hacked
					2017 FAFSA IRS Breach
					2017 WannaCry Ransomware
					2017 Petya Ransomware

Increasing Threat Profile



TAKE-AWAYS

- Cyber Risk profile is growing exponentially
- Cyber crime can harm you personally, professionally, and due to your privileged access to college data, your action or inaction can also impact students and the College
- Good security is EVERYONE's responsibility

Increasing Regulatory Requirements

- In addition to our need to protect students, parents, staff, faculty, and the college, we have growing legal and contractual requirements
- Many federal mandates now require policies, procedures, and breach disclosures related to Cyber Security



Increasing Cyber Security Requirements

- Gramm-Leach-Bliley Act (GLBA) - Cyber Security audits start in FY18 per ruling from the Department of Education
- Higher Education Act (HEA)
- Family Educational Rights and Privacy Act (FERPA)
- Student Aid Internet Gateway
- Payment Card Industry - Data Security Standards (PCI DSS)



Carthage's IT Security and Acceptable Use of Technology Policy was defined to clearly communicate these Cyber Security expectations and meet the requirement for a formal policy



Carthage's IT Security & Acceptable Use of Technology Policy



IT Security & Acceptable Use of Technology Policy

The policy documentation is posted on MyCarthage under Employees Tab, Carthage Policies

It will be effective November 1, 2017 for new content; updates and remediations must be completed by February 1



Information Systems Policy Information Security & Acceptable Use of Technology

PURPOSE

Carthage College is committed to maintaining reliable technology operations and protecting our students, faculty, employees, and other stakeholders from illegal or damaging actions by individuals, either knowingly or unknowingly. This policy is intended to keep sensitive information secure and ensure ongoing IT operations, while not imposing undue restrictions to Carthage's culture of openness, trust, and integrity. It is the responsibility of all Carthage employees and other constituents that have been given Carthage network accounts to understand these policies and to conduct their activities accordingly. The purpose of this policy is not to replace but to supplement existing laws, regulations, general codes of conduct, agreements, and contracts that are currently in place.

In support of its mission of teaching and learning, and within its institutional priorities and financial capabilities, Carthage College provides access to computing, network and information systems and services for students, faculty, and staff that are governed by this policy.

SCOPE

This policy applies to all users of computing resources owned or managed by Carthage College. Individuals covered by the policy include faculty and visiting faculty, staff, and student employees.

ware and software, less of the



Data Classification Framework

The Data Classification Framework was developed to aid users in appropriately protecting College data. The higher the classification level, the greater the required protection. Data must be consistently protected throughout its life cycle in a manner commensurate with its sensitivity and criticality. Policies regarding the storage and management of data, based on this *Data Classification Framework*, are outlined in the *IT Security & Acceptable Use of Technology* policy.

	Examples	Data at Rest	Data in Transit
Level 4 – Restricted Data that is required to be protected by applicable law or statute in the most stringent manner possible. In some cases, unauthorized disclosure or loss of this data would require the College to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual.	Data that is Restricted: Social Security Numbers, Credit Card Numbers, Human Subjects Data - personally identifiable health information used in research, and Data used to authenticate or authorize individuals to use electronic resources - passwords, keys, and other electronic tokens. Note: Carthage has introduced service providers to handle credit card transactions, so no office should ever need to store credit card numbers.	Store only in Carthage enterprise applications or on the S drive, with access restricted. If data has to live on your hard drive, your hard drive must be encrypted (using BitLocker for Windows operating systems; standard for Mac OS is under development)	All email must be encrypted using FIPS 140-2 standards. Additional software licensing is required to perform this encryption, and available thru LIS. LIS must encrypt interfaces



Policy Coverage

1.0 User IDs and Passwords



2.0 Device Security

3.0 Data Storage

4.0 Confidential Information

5.0 Deceptive, Unethical, Illegal Activities

6.0 System Performance

7.0 Intellectual Property & Copyrighted Material

8.0 Personal Use of Company-issued devices

9.0 Technology Acquisition

10.0 Detection & Notification of Breaches

11.0 Security Awareness

12.0 Compliance with Applicable Laws



User Ids and Passwords - Carthage Requirements

To be or not
to be, that is
the question.

2bon2btitq



- Follow good password practices
- Carthage will require 12 character minimum; min 1 numeric

Reset your password at <https://password.carthage.edu>

Use Multi-Factor Authentication when available

- Carthage requires Google 2-Step Verification to be turned on by all Faculty & Staff “Ask Albert” Article ID 1424
- Carthage will be turning on requirement for 2-factor authentication for VPN

Google 2-Factor Options



Get codes via text message

Google can send verification codes to your cell phone via text message. Your carrier's standard messaging rates may apply.



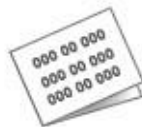
Backup phone numbers

Add backup phone numbers so Google has another way to send you verification codes in case your main phone is unavailable.



Want a phone call instead?

Google can call your cell or landline phone with your verification code.



Backup codes

You can print or download one-time use backup codes for times when your phones are unavailable, such as when you travel.



No connection, no problem

The Google Authenticator app for Android, iPhone, or BlackBerry can generate verification codes. It even works when your device has no phone or data connectivity.



Tired of typing verification codes?

Get a Google prompt on your phone and just tap **Yes** to sign in.

Get Help

- Use *Albert Article #1424 - How do I turn on Google's 2-Step Verification?*
- Stop by the Information Desk
- Attend the walk-in session during the Teaching & Learning Conference
- Ask for help when picking up your new PC (for those who are in this year's refresh cycle)



Policy Coverage

1.0 User IDs and Passwords

2.0 Device Security



3.0 Data Storage

4.0 Confidential Information

5.0 Deceptive, Unethical, Illegal Activities

6.0 System Performance

7.0 Intellectual Property & Copyrighted Material

8.0 Personal Use of Company-issued devices

9.0 Technology Acquisition

10.0 Detection & Notification of Breaches

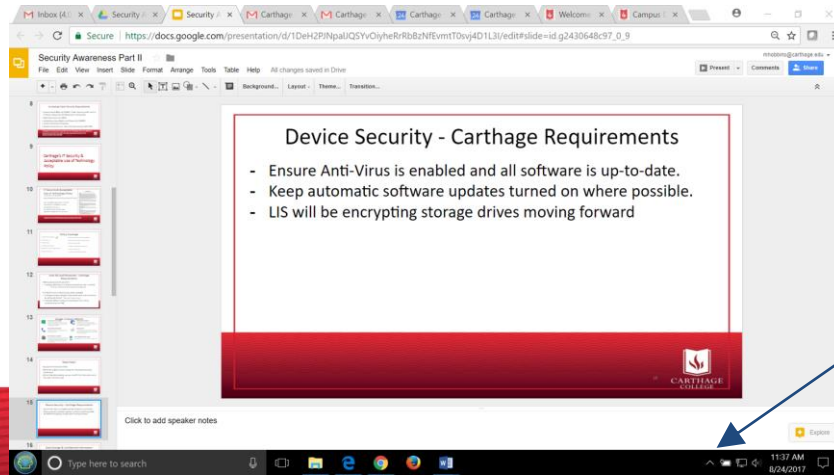
11.0 Security Awareness

12.0 Compliance with Applicable Laws



Device Security - Carthage Requirements

- Ensure Anti-Virus is enabled and all software is up-to-date.
- Keep automatic software updates turned on where possible.

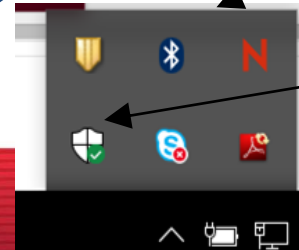


Click here

THEN ...

Check for software updates

check antivirus



For Macs, the icon is in upper right corner of your monitor

Device Security - Carthage Requirements



- Carthage will be enabling encryption on laptops and desktops
- Users of Carthage Protected data must secure computing devices with a password-protected screensaver, and lock the screen or log off when the device is unattended

Instructions for Screen Locking

1. Go to **Ask Albert**: <https://albert.carthage.edu/>
2. **Passwords and Security** section on the left.
3. Article titles & ID numbers below...

Albert Article ID#1472

Android Security

Albert Article ID#1474

iOS Security

Albert Article ID#1471

macOS Security

Albert Article ID#1473

Windows Security




Policy Coverage

1.0 User IDs and Passwords

2.0 Device Security

3.0 Data Storage 

4.0 Confidential Information 

5.0 Deceptive, Unethical, Illegal Activities

6.0 System Performance

7.0 Intellectual Property & Copyrighted Material

8.0 Personal Use of Company-issued devices

9.0 Technology Acquisition

10.0 Detection & Notification of Breaches

11.0 Security Awareness

12.0 Compliance with Applicable Laws



Data Storage & Confidential Information

- All Carthage data used for internal purposes must be stored in LIS-approved applications or LIS-approved storage drives
- G Suite for Education (ie Gmail; Google Docs) is the only authorized cloud data repository for individual or Carthage team storage of unstructured data for internal purposes
- If temporary local copies of data are needed, they must be uploaded to an LIS-approved storage drive on a periodic basis to minimize risk of loss
- Must use password-protected screen saver if using confidential data



Faculty Perspective – Data Classification Framework

The Data Classification Framework is intended to cover Carthage data. It does not prescribe your handling of the following:

- Syllabus and other materials you are developing for courses
- Course notes
- Your personal records about student progress ... but you are responsible to comply with FERPA requirements if your records meet FERPA definition
- Student work (student Intellectual Property)



Data Storage & Confidential Information

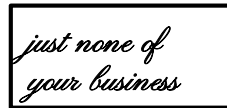
Level 4 - Restricted



Level 3 - Confidential



Level 2 - Internal



Level 1 - Public



	Data at Rest	Data in Transit
<p>Level 4 - Restricted</p> <p>Data that is required to be protected by applicable law or statute in the most stringent manner possible. In some cases, unauthorized disclosure or loss of this data would require the College to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual.</p>	<p>Store only in Carthage enterprise applications or on the S/I/O drive, with access restricted</p> <p>If data has to live on your hard drive, your hard drive must be encrypted (using Bitlocker for Windows operating systems; standard for Mac OS is under development)</p>	<p>Email must be encrypted using FIPS 140-2 standards. Additional software licensing is required to perform this encryption, and available thru LIS.</p> <p>LIS must encrypt interfaces</p>

Level 4 DATA: Social Security Numbers, Credit Card Numbers, Human Subjects Data, Passwords/tokens



	Data at Rest	Data in Transit
<p>Level 3 – Confidential</p> <p>Data that is required to be protected by applicable law or statute (e.g., FERPA, HIPAA), or which, if disclosed to the public could expose the College to legal or financial obligations, or which the College has decided to keep confidential. It includes personally identifiable information which if disclosed would create risk of criminal liability, loss of insurability, severe social, reputational, or financial harm.</p>	<p>Store only in Carthage enterprise applications, Google Team Drives, or on the S/I/O drive, with access restricted</p> <p>If data has to live on your hard drive, your hard drive must be encrypted (using Bitlocker for Windows operating systems; standard for Mac OS is under development)</p>	<p>Email sent to a non-Carthage domain must be encrypted using FIPS 140-2 standards. Additional software licensing is required to perform this encryption, and available thru LIS.</p>



EXAMPLES:

Academic records, health and medical records, personally identifiable information entrusted to our care that is not Restricted Use data, student financial aid information, disciplinary records, personnel records, applicant data, carthage id number

Presidential search details (while in process), Strategic Plan (while under development), alumni and donor information, course evaluations, financial budgets and plans, monthly financial management reports, unpublished financial information

	Data at Rest	Data in Transit
<p>Level 2 – Internal</p> <p>Information that would not cause material harm if disclosed, but is proprietary to the operation of the College, and should be made available to those with a need to know to perform their function effectively. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Internal information is not intended for public dissemination but may be released to external parties to the extent there is a legitimate business purpose.</p>	<p>Data should be maintained in Carthage enterprise applications or the S//I/O drive or Google Team Drives, with access only given based on appropriate role. Reminder: 2-factor authentication is required for Google.</p>	<p>Email does not require FIPS 140-2 encryption</p> <p>LIS will put appropriate controls on interfaces</p>

it's not a secret its just none of your business



	Data at Rest	Data in Transit
<p>Level 1 – Public</p> <p>Carthage.edu external web site. Recruiting information, campus maps, building layouts, published information about the college, published research, course catalog, directory information about students who have not requested FERPA block, faculty and staff directory information</p>	<p>While the data can be freely shared, definitive master versions should be maintained in Carthage enterprise applications or the S/I/O drive or Google Team Drives. Update access to master versions still needs to be limited to appropriate parties. Reminder: 2-factor authentication is required for Google.</p>	<p>No Email restrictions</p> <p>LIS will put appropriate controls on interfaces to prevent tampering</p>



EXAMPLES: Carthage.edu external web site. Recruiting information, campus maps, building maps, published information about the college, published research, course catalog, directory information about students who have not requested FERPA block, faculty and staff directory information

Collaborating with other Educational Institutions, Affinity Groups, etc

- Confidential Data (Level 3) If sharing Confidential data, the storage method needs to meet Carthage standards of confidentiality. This would mean that Carthage could host in Google and share access. Or a partner could host our data if they are protecting the data.
- If Confidential Data is sent to a partner in email, we would need to encrypt it.
- If sharing non-confidential Internal data (Level 2) there aren't restrictions to where it is kept, but access can only be open to appropriate individuals based on the initiative



Policy Coverage

1.0 User IDs and Passwords

2.0 Device Security

3.0 Data Storage

4.0 Confidential Information

5.0 Deceptive, Unethical, Illegal Activities

6.0 System Performance

7.0 Intellectual Property & Copyrighted Material

8.0 Personal Use of Company-issued devices

9.0 Technology Acquisition

10.0 Detection & Notification of Breaches

11.0 Security Awareness

12.0 Compliance with Applicable Laws

LEGAL and ETHICAL Behavior

Employees must comply with all laws and not engage in activity that will negatively impact the IT environment for the College



Policy Coverage

1.0 User IDs and Passwords

2.0 Device Security

3.0 Data Storage

4.0 Confidential Information

5.0 Deceptive, Unethical, Illegal Activities

6.0 System Performance

7.0 Intellectual Property & Copyrighted Material

8.0 Personal Use of Company-issued devices ✓

9.0 Technology Acquisition

10.0 Detection & Notification of Breaches

11.0 Security Awareness

12.0 Compliance with Applicable Laws

**Reasonable personal use of college-owned devices is acceptable
as long as it doesn't impact college functions**



Policy Coverage

1.0 User IDs and Passwords

2.0 Device Security

3.0 Data Storage

4.0 Confidential Information

5.0 Deceptive, Unethical, Illegal Activities

6.0 System Performance

7.0 Intellectual Property & Copyrighted Material

8.0 Personal Use of Company-issued devices

9.0 Technology Acquisition



10.0 Detection & Notification of Breaches

11.0 Security Awareness

12.0 Compliance with Applicable Laws

Acquisition of information software and hardware must be coordinated through LIS to ensure they are integrated, secured, tested, deployed, and managed through ongoing backups, maintenance, upgrades, and eventual decommissioning.



Policy Coverage

1.0 User IDs and Passwords

2.0 Device Security

3.0 Data Storage

4.0 Confidential Information

5.0 Deceptive, Unethical, Illegal Activities

6.0 System Performance

7.0 Intellectual Property & Copyrighted Material

8.0 Personal Use of Company-issued devices

9.0 Technology Acquisition

10.0 Detection & Notification of Breaches

11.0 Security Awareness



12.0 Compliance with Applicable Laws

Employees must participate in annual security awareness training



Wrap-Up



What's Next?

- LIS will execute the anti-phishing exercise portion of the Security Awareness training to you
- LIS will provide desktop encryption
- Upcoming Specialty Training Sessions
 - Email Encryption - for individuals that need to email confidential information
 - Payment Key Industry (PCI) - for credit card handling
 - VPN (Global Protect) - Multi-Factor Authentication
- Moving forward, LIS will provide ongoing Anti-Phishing training campaigns and Updated Annual Security Awareness Training

Your Checklist

- ___ Reset your password if <12 characters [*password.carthage.edu*]
- ___ Turn on your Screensavers Albert Articles: MacOS-1471;Android-1472;Windows-1473;IOS-1474
- ___ Verify anti-virus is up-to-date
- ___ Turn on Google 2-step authentication [Ask Albert” Article ID 1424]
- ___ Validate you are connecting to Carthage Secure WiFi if possible
- ___ Review the *IT Security and Acceptable Use of Technology Policy*
- ___ Complete the Security Awareness Questionnaire when you receive the link and reference materials

