Welcome

Carnegie Mellon University
Information Security Office

October 24, 2016

Our Shared Responsibility

National Cyber Security Awareness Month
Opening Remarks
  – Dr. Rodney McClendon, V.P. Operations
Emerging Cyber Threats
Introduction to BC/DR Planning
Strengthening Authentication with 2FA
Improving Password Management
Emerging Cyber Threats

Mary Ann Blair, Director, Information Security Office
Threat Actors

- **Nation States**
  - Nationalistic motivation
  - Espionage for economic and military advantage (Advanced Persistent Threat), disruption (Stuxnet)

- **Cyber Criminals**
  - Financial motivation
  - Extortion (ransomware), theft (redirect direct deposit), profit (sale of personal information)

- **Hacktivists**
  - Political or ideological motivation
  - Embarrass (deface, information disclosure), disrupt (denial of service)

- **Script Kiddies**
  - Ego motivation
  - Test their skills (canned hacks)

- **Insiders**
  - Various motivation
  - Help (click), revenge (logic bombs)
Threat Actor Workflow

Identification, Reconnaissance, & Enumeration
- Select the target: known (intentional) vs vulnerable (opportunistic)
- Learn about the target (websites, press releases, network probes, staff directories)

Exploitation
- Create the exploit (construct scam message, malware, etc)
- Deliver the exploit (email, infected websites)
- Trigger the exploit (human execution (reply, click, open), software or hardware)

Command & Control
- Create a point of presence (additional backdoors to maintain persistence)
- Establish on-going two-way communication

Action on Objective
- Data exfiltration, modification, and/or destruction
- Expand the local foothold
- Attack another target (phish others, attack others ‘anonymously’)
Sample Threats

- Advanced Persistent Threat (APT)
- Ransomware
- Spear Phishing
“The hackers tried to cloak the source of the attacks on The Times by first penetrating computers at United States universities and routing the attacks through them, said computer security experts at Mandiant, the company hired by The Times. This matches the subterfuge used in many other attacks that Mandiant has tracked to China.”

Source: http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?_r=0
  – November 21, 2014 – FBI notifies Penn State of breach
  – May 15, 2015 breach publicly announced coincident with engineering school going off-line for the weekend to rebuild computers
• “Chinese hackers attack University of Virginia email, cause IT shutdown” – Examiner. August 14, 2015.
  – June 2015 – FBI notifies UVA of breach
  – August weekend outage; email, Student Information Systems, Collab site,
  – Emergency notification via fire alarm sirens, social media accounts, and “Alert Now”
Characteristics of APT

• Extremely targeted attack
• Nation states with resources
• Sophisticated, blended attacks
  – Spear phishing to gain credentials
  – Custom malware (no signatures)
  – Sophisticated evasion techniques
  – Lateral movement, deeply imbedded
  – Extreme Stealth
• Patient and relentless; willing to wait months or years for pay-off; resilient; adaptive
• Continuous monitoring; command and control
• Often aimed at R&D, commercial and defense payloads
Response to APT

- Engage law enforcement and outside experts
- Trace and detect ALL the footholds before ANY remediation to avoid driving attackers further under ground
- Use out of band communication – emails are monitored
- Significant, “big bang” remediation efforts
- Data breach notification and reputation management (constituents, sponsors, threat actors)
Ransomware

Your personal files are encrypted!

Your important files encrypted produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Ransomware

- “Fastest growing” malware
- Impacts all operating systems
- Infects networked storage & removal media
- Layered impacts including data breach and theft

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

PSU Ransomware Email Attack
Author: Michelle Malkasian, Office of Information Technology
Posted: March 18, 2016

Over the past several hours, Portland State University has been subject to a large-scale email attack. You may receive an email asking you to download an invoice attachment. It is extremely important that you do not download this file.
Your files are encrypted.
To get the key to decrypt files you have to pay 500 USD. If payment is not made before 20/07/15 - 19:41 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:

167h 56m 11s

Your system: Windows XP (x32) First connect IP: (Redacted) Total encrypted 330 files.

Refresh Payment FAQ Decrypt 1 file for FREE Support

We give you the opportunity to decipher 1 file free of charge! You can make sure that the service really works and after payment for the CryptoWall program you can actually decrypt the files.

Your file is successfully decoded. You can download it

Download decrypted file
Response to Ransomware

- Prevent it with basic security hygiene
- Detect and interrupt it ASAP
- Restore from “real” back-ups
- Restore from other sources (e.g., sent email)
- Use a decryption tool if available
- Pay the ransom
  - Bitcoin account or Bitcoin broker service
  - Prepare in advance - the clock is ticking
  - Can be cheaper than all of the above responses
“highly targeted phishing aimed at specific individuals or groups within an organization. …spear phishing makes the use of information about a target to make attacks more specific and “personal” to the target.”

“Spear phishing significantly raises the chances that targets will read a message that will allow attackers to compromise their networks. “

*Spear-Phishing Email: Most Favored APT Attack Bait.* Trend Micro. 2012.
From: Farnam Jahanian via Dropbox [mailto:official@andrew.cmu.edu]
Sent: Thursday, March 17, 2016 10:10 PM
To: Recipient <no-reply@dropboxmail.com>
Subject: Farnam Jahanian (official@andrew.cmu.edu) has sent you a document

Farnam Jahanian (official@andrew.cmu.edu) has invited you to view the following documents via Dropbox shared folder.

To view the document, please click here or view folder below and sign in your email and password to continue to Dropbox shared folder.

NOTE: You are accessing a highly secured important document.

Enjoy,
- The Dropbox Team
To view the shared document, you are required to Login with your email address below:

Email Address: 

Email Password: 

Sign in
• Many diagnosis & report phish
• Time is of the essence for incident response
• No visibility of off-campus clicks
• No blocking in effect off-campus
• Victims must self-identify or wait to be identified from malicious network traffic
• Anti-virus/block list timing can send recipient notification to spam folders
• Additional 5 victims came forward after reading a follow-up massmail that included info about this and other scams
Use of Phished Credentials

- Additional reconnaissance
- Access employee self-service to change or redirect direct deposit
- Launch the next wave of phishing
- Learn password composition strategy to brute force victim’s other accounts (identity theft)
Response to Spear Phishing

- Block sender
- Block destination(s)
- Notify each recipient
- Identify victims
- Secure accounts
- Secure computers
- Check for account use
- Check for data loss
- Rebuild
- Catch the next wave
- Simulated phishing tests
- Service improvements (prevent delivery)

Subject: Important Phishing Notice - Please Read

Our records indicate you may have received a malicious "phishing" email. A sanitized copy of the malicious email is included below for your reference.

The phishing message was sent to the following address:

Recipient_name@cmu.edu

"Phishing" is the practice of sending emails which often look legitimate and encourage recipients to click a link or respond via email and inadvertently provide information, often a username and password, to an unauthorized third party.

WHAT YOU NEED TO DO:
If you think you may have clicked the link in the email referenced below and subsequently entered your username and password, please contact the Information Security Office immediately at iso-ir@andrew.cmu.edu or 412-268-2044.

***Below is a sanitized copy of the malicious email for your reference***

*** End of sanitized malicious email ***

Thank you,
1. Secure Your Account & Password
   - Long and/or complex
   - Don’t share or insecurely write/store
   - Change periodically based on risk scenarios
   - Avoid automatic logons
   - Don’t reuse
   - Change default passwords
   - Don’t ask, don’t tell
   - Report concerns promptly to iso-ir@andrew.cmu.edu
2. Secure Your Computer
   - Configure automatic updates
   - Use anti-virus
   - Password protect computer
   - Password protect screen saver
   - Turn on the firewall
   - Limit privileged account use
   - Secure and test your backups
   - Report concerns promptly to iso-ir@andrew.cmu.edu
3. Don’t Take the Bait
   - Learn to detect phishing
   - Report suspicious email to iso-ir@andrew.cmu.edu
   - Verify unexpected or odd email before clicking or opening attachments (especially true for folks who routinely receive attachments from a variety of internal and external senders)
   - Stay alert for other types of social engineering
   - Challenge, courteously
   - Report concerns promptly to iso-ir@andrew.cmu.edu
Thank you!
Introduction to Business Continuity and Disaster Recovery Planning

Melanie Lucht, Senior Manager, DR/BC Services
“Provide the guidance, tools, and governance commensurate with the strategic mission and risk tolerance of the University and its divisional units so that they may continue to provide critical services in the event of a disaster or significant business disruption.”
Three Objectives

PARTNER

PROVIDE

MANAGE
Three Objectives

PAINLESS

MORE PAINLESS

MORE
Capability of an organization to continue delivery of critical services at an acceptable level following a disaster or significant business disruption (addresses actions taken in the event of a loss to people, facility, technology, and supplier)

All Hazard Approach
Disaster Recovery
Subset of Business Continuity that focuses on the collection of resources and activities to re-establish information technology services at an alternate site following a disruption of IT services in the event of a significant business disruption or disaster.

All Hazard Approach
Benefits of Business Continuity

- Goal of Business Continuity = “To ensure… (insert institutional mission and/or strategy here)”
- Expectations of preparedness
- Vested interest in the success of organizational continuity and resiliency
- Identifies potential risks to achieving recovery
- Bridges the knowledge gap
- Peer Benchmarking
- Understand the inner workings of the entire organization
When Does BC or DR get activated?

Business Continuity Exposure Distribution

"tail events"
CMU Risk Management Continuum

Risk Management

What could happen?
- Identify hazards and opportunities
- Assess impact & likelihood
- Make risk decisions
- Implement controls
- Watch for changes

Emergency Response

What if it happened?
- Stabilize conditions following a risk event and minimize negative effects

Business Continuity

What next?
- Reestablish sufficient services to permit continued mission-essential operations following a risk event
Business Continuity Lifecycle

- Business Impact Analysis
  - Data gathering and recovery requirements

- Risk Assessment/Gap Analysis
  - Assess potential risks and gaps between recovery requirements and recovery capabilities
  - Decide whether to remediate or accept risks

- Plan Development/Update
  - Create and maintain Business Continuity Plans that address actions to be taken in the event of a loss to facility, technology, people, and supplier

- Plan Exercising & Continuous Improvement
  - Exercise Plans to validate feasibility
DR/BC Steering & Advisory Committee

- **Role**
  - Meets quarterly to provide strategic oversight of program goals;
  - Responsible for acceptance of program deliverables;
  - Provide disciplinary expertise and direction to the scope, approach, and timing of DR/BC initiatives

- **Decision-making Authority**
  - Can change schedules, tasks, budget, or resources that affect overall program
  - Provide recommendations to Executive Management

- **Executive Sponsors**
  - Steve Huth, Senior Advisor to Interim CIO
  - Lisa Krieg, Director of Enrollment Services

- **Members**
  - David Baisley, Mary Ann Blair, - Computing Services
  - Liz Milavec - Finance
  - Ann Mathias – Research Administration
  - Greg Billy – Campus Services & Risk Initiatives
  - Madelyn Miller - Environmental Health & Safety
  - Keith Webster – Dean of University Libraries
  - Roy Farkas, Facilities Management Services
The DR/BC Services Multi-Year strategy is focused on the prioritization of Administrative organizations that bear the greatest potential risk impact in the event they are unable to recover following a disaster or significant business disruption.
Strategic Framework and Risk Impact

Risk Impacts that have the potential to disrupt the framework of the Strategic Plan:

- Life/Health Safety
- Financial/Revenue Generation
- Reputational
- Legal/Compliance
- Operational
**Administrative Organizations by Risk Impact**

**Key Principles:** Ensure Safety of University Community, Protect University Reputation, Transaction Processing and Service to Existing Customers, and Provide Core Services

![Diagram of Administrative Organizations by Risk Impact](image)

- **Life/Health Safety Impact**
  - EH&S
  - Facilities Mgmt
  - University Police
  - Health Services
  - Human Resources
  - Communications
  - Student Affairs

- **Revenue Generation/Financial Impact**
  - Finance
  - Research Admin
  - Undergraduate Admission
  - Enrollment Services
  - University Advancement
  - Investment Office
  - Center for Tech Transfer

- **Legal/Compliance Impact**
  - Office of General Counsel
  - Information Security Office
  - Government Relations
  - Risk Management

- **Operational Impact**
  - Athletics
  - Computing Svcs (partial)
  - CDFD
  - Campus Services
  - University Audit Svc
  - Vice Provost for Education
  - Executive Offices
  - Real Estate

**2013 - 2018**

Green = In BC Program
Purple = Outreach Initiated
Black = Outreach Not yet Initiated
Business Continuity Initiative Resources

**DR/BC Services**
- Educate and Train
- Lead and Guide
- Coordinate Execution of BC Initiative
- Conduct Risk Assessment and Gap Analysis
- Coordinate Leadership Review and Validation of Recovery Priorities
- Ongoing Support and Consultation

**Sponsor (SPOC)**
- Liaison between DR/BC Services and Division/Dept
- Expert Level of Knowledge of Division/Dept
- Identifies Stakeholders
- Provides Overall Support and Guidance

**Plan Owner**
- Manages/Leads Business Function
- Assigns Plan Administrator(s)
- Ownership/Accountability of Plan
- Annual Review and Approval of BC Plan
- Supports/Participates in Annual BC Exercise

**Plan Administrator(s)**
- Designated by Plan Owner
- Works with DR/BC Services through the BC Lifecycle (BIA, Planning, Exercises)
- Electronically Submits Plan to Owner for Review and Approval
- Ongoing Business Function and Plan Maintenance

**Time Commitment:**
1. Training = 1 hour
2. BIA = 1-3 hours
3. Plan Development & Review = 1 hour
4. Plan
5. Plan
## Business Continuity – 2016 KPI’s

### Business Continuity Plans By Organization

<table>
<thead>
<tr>
<th>Organization</th>
<th>Total Plans</th>
<th>Plans in Development</th>
<th>Plans Approved</th>
<th>Exercises 2016</th>
<th>Progress/Status since 8/16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campus Design &amp; Facilities Development</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Campus Services</td>
<td>8</td>
<td>5</td>
<td>3</td>
<td>3 in October</td>
<td>1 Plan Approved</td>
</tr>
<tr>
<td>Computing Services</td>
<td>28</td>
<td>9</td>
<td>19</td>
<td>7 Exercises from July-Oct</td>
<td>8 New Plans 7 Plans Approved</td>
</tr>
<tr>
<td>EH&amp;S</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>July</td>
<td></td>
</tr>
<tr>
<td>Enrollment Services</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2 Plans in April/May</td>
<td></td>
</tr>
<tr>
<td>Facilities Management</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>June</td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td>14</td>
<td>0</td>
<td>14</td>
<td>5 Plans in April</td>
<td></td>
</tr>
<tr>
<td>Health Services</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>August</td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>7</td>
<td>6</td>
<td>1</td>
<td>1 in October</td>
<td>1 Plan Approved</td>
</tr>
<tr>
<td>Marketing &amp; Communications</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>March</td>
<td></td>
</tr>
<tr>
<td>Office of General Counsel and UCO</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real Estate</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student Affairs (DOSA)</td>
<td>8</td>
<td>0</td>
<td>8</td>
<td>August</td>
<td></td>
</tr>
<tr>
<td>Student Affairs Operations</td>
<td>7</td>
<td>0</td>
<td>7</td>
<td>November</td>
<td></td>
</tr>
<tr>
<td>University Advancement</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>University Police</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>August</td>
<td></td>
</tr>
<tr>
<td>University Libraries</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>May</td>
<td></td>
</tr>
<tr>
<td>Research Administration</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>2 Plans in April</td>
<td></td>
</tr>
<tr>
<td>Undergraduate Admission</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>105</strong></td>
<td><strong>22</strong></td>
<td><strong>83</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**2016 Plan Count**
- February: 67 Plans
- May: 68 Plans
- August: 97 Plans
- October: 105 Plans
Fusion Risk Management

- Cloud-Based Third-Party Solution
- Plan Development/Management
- Email Notifications and Reminders
- Track, Manage, Monitor Risks
- Plan and Manage Exercises
- Real Time Dashboards and Reports
- Prioritization of Recovery
- Accessible on any device/browser

October 2016 - 317 Licensed Users

Informed Decision Making
Coming Soon...

Strengthening Authentication with 2fa

Deborah Schill, Assistant Director, Identity Services
ID and password pair is the sole means of authenticating access

- Email
- File storage
- Enterprise applications (including human resource, financial, and student data)
- Sponsored project information (including conflict of interest information)
- Library subscriptions
- Licensed software downloads
IDs and passwords are vulnerable to attack and disclosure

- Attacker use of compromised accounts includes attempts to change employment direct deposit instructions, launch of additional phishing attacks and reconnaissance and exploitation of the university network and computers.
- Identification of root cause for credential loss is often costly. For this reason, root cause is not always determined and metrics are incomplete and under-represented.

The trend in phishing attacks and their success is undeniable.
Current Mitigations

- User awareness via email
- Web content
- Simulated phishing tests
- Published guidelines for securing passwords and computers
- Inbound email filtering
- System and application monitoring
- Timely incident response including:
  - Network and response blocking (where we can)
  - Victim notification
  - Forensic analysis
  - Forced password resets when account compromise is known or suspected

...but it is not enough!
Don’t forget to Report Concerns to the ISO

[Report Concerns webpage screenshot]

- Suspect a computer you use for University related work or study is:
  - Compromised (un-authorized interactive access)
  - Infected by viruses, worms, or other malware
  - Attacking other systems
  - Mis-configured leading to security vulnerability or negative impact on University computing infrastructure
  1. Follow the [Procedure for Responding to a Compromised Computer](#).
  2. Email iso-ir@andrew.cmu.edu or call the ISO at (412) 268-2044.

- Suspect a computer used for University work or study has committed a security breach or is under attack
  Email iso-ir@andrew.cmu.edu or call ISO at (412) 268-2044 and include relevant:
  - timestamps (including timezone)
  - hostnames or IP addresses
  - network device or service access logs
  - contact information

- Reporting an email scam or phishing attempt
  Email iso-ir@andrew.cmu.edu or call ISO at (412) 268-2044 and include:
  - Email header information
  - Email subject line Phishing Attempt
  If you clicked on a phishing email link or attachment, follow the [Procedure for Responding to a Compromised Computer](#)

- Reporting that you may have been phished
  Follow the instructions at [I Might Have Been Phished, What Do I Do?](#)
Potential Proactive Tactics

ADDITIONAL AUTHENTICATION FACTOR
Add a factor beyond something that is known and can be easily disclosed.

REQUIRE REGULAR PASSWORD CHANGE
May be less secure overall if users write down or create guessable passwords to remember them.
People are easily tricked into disclosing what they know and they often don’t even remember disclosing the information.

An additional factor, such as something they are (a biometric) or something they have (a smartphone or token) addresses this weakness.
What is Two-Factor Authentication

Requires use of two of the three authentication factors.
Something only the user:
1. Knows (e.g. password, PIN, secret answer)
2. Has (e.g. ATM card, mobile phone, hard token)
3. Is (e.g. biometric – iris, fingerprint)

Most Common Example – Automated Teller Machine

TWO-FACTOR AUTHENTICATION

Insert bank card (Something you have)
Provide PIN (Something you know)
Receive money (Access)
Security risks associated with reliance on passwords alone is well known and widely discussed. Based on this risk, a shift to multi-factor authentication is under way in the federal government, across industry and in higher education.

- Consumers are increasingly provided options for multi-factor authentication. Examples: Google 2-step Verification, Facebook login approvals, and Bank of America’s SafePass

- Change primarily a result of phishing attacks aimed at changing direct deposit instructions. Examples: Boston University (13 faculty paychecks stolen), University of Iowa, Ohio State University, Virginia Tech, Penn State, Duke, and UC Berkeley
Significant growth in Phishing attacks and users who fall victim to these attacks requires a substantial increase in work effort.

- Jul 2015 - Jul 2016: average phishing attacks grew from 3 to 20 per month
- Jul – Dec 2015: approximately 20 recipients responded to a Phishing attack
- Jan – Jul 2016: approximately 116 responded to a Phishing attack
CURRENT STATUS

IN PRODUCTION

• Risk Based Role
  o Select VPN*
  o Citrix/My OTP Apps
  o Windows AD Password Tool

• Mandatory for All
  o Grouper
  o Credential Management
  o NetReg

*Two Factor Required since May 2007
Two-Factor Authentication will be available to the campus community by the end of 2016.

- Self-enrollment application
- Documentation and service materials
- Availability to demo and answer questions
Self-Service Enrollment Features

- Easily enroll your devices (smartphone, tablet)
- Re-activate when you get a new phone quickly to ensure minimal downtime
- Andrew ID + Card ID number for added enrollment protection
DUO EXPERIENCE

1. Log into application that is configured for Duo
2. Sign in with Andrew credentials at login.cmu.edu
3. Prompted for either Duo Push or Duo Token
4. Send Push to phone OR enter passcode
5. Start using application(s)
QUESTIONS
Improving Password Management

Laura Raderman, Policy and Compliance Coordinator, ISO
• How many passwords do you have?

• Are they all different?
  – How different?
  • Summer2016 vs Autumn2016?
• Picking a password can be difficult
  – Multiple sites have different rules – what may be acceptable on one site is unacceptable on another
    • Biggest culprit: sites that don’t accept special characters
  – Very strong passwords generally aren’t very memorable
    • buz%vG9X#paC3s
Password Managers!

- Generate and store your passwords
  - You don’t even have to think up a new password!
• Passwords are protected by a “master” password.
  – This is the password you will have to remember (you can still have the manager generate it for you if you want)
• The master password is used to encrypt all of your other passwords
  – Most are using AES256 with PBKDF2 (Password Based Key Derivation Function 2)
Master Passwords

- Select a very strong master password
  - All managers support changing it should you want/need to

- New NIST Recommendations
  - At least 8 characters
  - Not in a dictionary
  - Not in previously compromised account databases

- ISO’s Recommendation
  - Long (16+ character) phrase
http://xkcd.com/936/

Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
DO NOT FORGET YOUR MASTER PASSWORD!
Storage Options

- Offline storage
- Online storage

- Both are secure with our recommendations, but your risk tolerance may differ!
  - If you don’t sync/store online – BACKUP your file(s)!
Specific ISO Recommendations

- 1Password
- KeePass
- LastPass

ISO evaluated design at a high level for security of passwords
- It’s OK to store your Andrew password in these!

CMU DOES NOT support these
- https://1password.com
- Both an online and a desktop/mobile application
  - Both are secure!
- Not free
  - $64.99 for the “standalone” version (upgrades have been less in the past – usually ~$35 every 3-4 years)
  - $2.99/mth billed annually ($35.88/yr) for online
• Standalone version offers syncing through Dropbox, iCloud, file folder (including file shares)  
  – Syncing is not required!
• Standalone version is not compatible with Linux
• Online version supports offline caching (via applications), but is primarily online
• Browser integration with all major browsers
• **Watchtower/ Security Audit**
  – Lets you know about password breaches – like Yahoo’s or compromised private server keys
  – Points out weak or duplicate passwords
• Offline storage only
  – Plugins (not evaluated) for syncing capabilities: (Dropbox, Google Drive, OneDrive, SCP, SFTP, S3)
  – Don’t forget to BACKUP!

• Open Source

• Linux, OSX support via Mono, Windows support via .NET.

• Ports (not evaluated) for mobile devices
• Generates passwords
• Free!
• Browser integration only via plugins (not evaluated)
• Online “only”
  – Local password cache
• Supports 2-factor soft token authentication (including Duo!) for free
  – 2-factor hard token authentication available with Premium subscription
• Free for most features. Premium features $12/year.
• Native Browser integration for all major browsers
• Linux support
• Password Auditing
• Mobile applications
Welcome to Cyburgh, PA

Careers in Cyber Security
In Brief: Pittsburgh’s Resurrection
Casting off its gritty, industrial reputation, Pittsburgh has become something of a hub for artists, techies, and food enthusiasts. ...
• Cybersecurity was born here!
• Academia, Government, Industry with a strong foothold
• Evolution cannot end...or we will end up next to the T-Rex in Carnegie Museum
• If we don’t do this, someone else will
• 1.5 million jobs shortfall projected by 2019, Symantec’s CEO
• Jobs growing at a rate of 36.5% through 2022
• Only 11% of world’s info sec workforce are women according to Women’s Society of Cyberjitsu
• Pipeline
• Recruiting
• Retaining
• Training
Summer Craze Fowler – moderator

Laura Raderman - Policy and Compliance Coordinator, ISO (Information Security Analyst)

Jon Zeolla - Senior Information Security Engineer, ISO (Network Security Administrator)

Deana Shick - Member of Technical Staff, CERT (Cyber Crime Investigator)

Ted Pham - Manager of Security Engineering and Operations, ISO (Security Architect)

Brian Gray - Senior Information Security Engineer, ISO (Penetration Tester)

Melissa Lucas - Information Security Engineer, ISO (Security Software Developer)

Mary Ann Blair - Director, Information Security Office, ISO (CISO)
Gmail Security Tools for Personal or Google Apps for Education Users

How To Keep Your Email Off WikiLeaks

Ted Pham, Manager of Security Engineering & Operations, Information Security Office
Terminology

Personal Gmail
• @gmail.com

GAFE – Google Apps for Education
• @andrew.cmu.edu
Login Page: GAFE Login.cmu.edu

Web Login

AndrewID
Password

Login

Warning: The URL for this page should begin with https://login.cmu.edu. If it does not, do not fill in any information, and report this site to it-help@cmu.edu.

About | Change Password | Forgot Password?
Login Page: GAFE Login.cmu.edu - Phished

Carnegie Mellon University
Information Security Office

Login.cmu.edu

Web Login

AndrewID
Password

Warning: The URL for this page should begin with https://login.cmu.edu.
If it does not, do not fill in any information, and report this site to it-help@cmu.edu.
Login Page: GAFE Login.cmu.edu - Real

Web Login

AndrewID
Password
Login

Warning: The URL for this page should begin with https://login.cmu.edu. If it does not, do not fill in any information, and report this site to it-help@cmu.edu.

About | Change Password | Forgot Password?
Real Login Page URL starts with: https://accounts.google.com
Private Security Group Says Russia Was Behind John Podesta’s Email Hack

How Russia Pulled Off the Biggest Election Hack in U.S. History
Responding to a Phish: Change Password

Carnegie Mellon University
Information Security Office

CMU Credential Management

Change Password

Logged in as: t-telamon

Select the password you want to change:
- Andrew Password
- Andrew Google Apps @ CMU Password

To ensure success, please follow these requirements when selecting your password:

Must Contain:
- a minimum of 8-characters (one uppercase, one lowercase, one number, one special character)

Cannot Contain:
- known personal information
- last five passwords
- four or more occurrences of same character*
- a Dictionary word* (after removing non-alpha characters)
*Does not apply to passwords that are more than 19 characters in length (e.g., a passphrase).

Current Password: 
New Password: 

Password strength:

Confirm Password: 

Change Password

You are missing required data or have errors
Responding to a Phish: Report It

Report Concerns

<table>
<thead>
<tr>
<th>CONCERN TYPE</th>
<th>REQUIRED ACTION(S)</th>
</tr>
</thead>
</table>
| Suspect a computer you use for University related work or study is:  
- Compromised (un-authorized interactive access)  
- Infected by viruses, worms, or other malware  
- Attacking other systems  
- Mis-configured leading to security vulnerability or negative impact on University computing infrastructure | 1. Follow the Procedure for Responding to a Compromised Computer  
2. Email iso-ir@andrew.cmu.edu or call the ISO at (412) 268-2044. |
| Suspect a computer used for University work or study has committed a security breach or is under attack | Email iso-ir@andrew.cmu.edu or call ISO at (412) 268-2044 and include relevant:  
- timestamps (including timezone)  
- hostnames or IP addresses  
- network device or service access logs  
- contact information |
| Reporting an email scam or phishing attempt | Email iso-ir@andrew.cmu.edu or call ISO at (412) 268-2044 and include:  
- Email header information  
- Email subject line Phishing Attempt  
If you clicked on a phishing email link or attachment, follow the Procedure for Responding to a Compromised Computer |
| Reporting that you may have been phished | Follow the instructions at I Might Have Been Phished, What Do I Do? |
Google Security Checkup

Control, protect, and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you.

- **Sign-in & security**
  - Control your password and account-access settings.
  - Signing in to Google
  - Device activity & notifications
  - Connected apps & sites

- **Personal info & privacy**
  - Manage your visibility settings and the data we use to personalize your experience.
  - Your personal info
  - Manage your Google activity
  - Ads Settings
  - Control your content

- **Security Checkup**
  - Protect your account in just a few minutes by reviewing your security settings and activity.
  - GET STARTED

- **Privacy Checkup**
  - Take this quick checkup to review important privacy settings and adjust them to your preference.
Next, please review the devices connected to your Google Account. Let us know if any of these devices look unfamiliar to you, and we'll work together to ensure no one else has access to your account. Learn more.

<table>
<thead>
<tr>
<th>Device</th>
<th>Current Location</th>
<th>Last Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Pittsburgh, PA, USA</td>
<td>CURRENT DEVICE</td>
</tr>
<tr>
<td>Windows</td>
<td>Bengaluru, Karnataka, India</td>
<td>September 29, 10:43 PM</td>
</tr>
<tr>
<td>Browser</td>
<td>Firefox 49.0</td>
<td>Bengaluru, Karnataka, India</td>
</tr>
<tr>
<td></td>
<td></td>
<td>September 29, 10:43 PM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hong Kong</td>
</tr>
<tr>
<td></td>
<td></td>
<td>September 29, 10:43 PM</td>
</tr>
<tr>
<td>Samsung Galaxy S6</td>
<td>United States</td>
<td>September 29, 10:41 PM</td>
</tr>
<tr>
<td>Windows</td>
<td>Pittsburgh, PA, USA</td>
<td>September 15, 10:37 AM</td>
</tr>
<tr>
<td>Linux</td>
<td>Pittsburgh, PA, USA</td>
<td>September 12, 1:23 PM</td>
</tr>
</tbody>
</table>

**Looks good**  **Something looks wrong**
Logout Other Sessions

Carnegie Mellon University
Information Security Office

Mail ▼

COMPOSE

Inbox (7)
Starred
Sent Mail
Drafts
More ▼

Computing Services
Andrew Password Changed - You have successfully changed your ANDREW password. This is it.
Oct 21

Computing Services
Account Expiration Notice - TO: Theodore Pham (sponsor) t-telamon t-telamon (sponsored affiliation)
Jun 23

Computing Services
Account Expiration Notice - TO: Theodore Pham (sponsor) t-telamon t-telamon (sponsored affiliation)
Jun 16

Computing Services
Computing Services Welcomes you to Carnegie Mellon - Computing Services Welcomes you the
6/27/15

Gmail Team
Tips for using your new inbox - Hi t-telamon Welcome to your Gmail inbox Save everything with
6/27/15

Gmail Team
The best of Gmail, wherever you are - Hi t-telamon Get the official Gmail app The best features c
6/27/15

Gmail Team
How to use Gmail with Google Apps - Hi t-telamon Work smarter with Gmail and Google Apps M
6/27/15

Using 0 GB

Program Policies
Powered by Google

Last account activity: 5 minutes ago
Details
### Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. [Learn more](#)

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Location</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Browser, mobile, POP3, etc.)</td>
<td>* United States (PA) (128.237.193.13)</td>
<td>11:34 am (6 minutes ago)</td>
</tr>
<tr>
<td>Browser (Safari)</td>
<td>United States (PA) (128.237.193.13)</td>
<td>11:29 am (10 minutes ago)</td>
</tr>
<tr>
<td>Browser (Safari)</td>
<td>United States (PA) (128.237.193.13)</td>
<td>11:11 am (29 minutes ago)</td>
</tr>
<tr>
<td>Browser (Safari)</td>
<td>United States (PA) (128.237.193.13)</td>
<td>10:48 am (52 minutes ago)</td>
</tr>
<tr>
<td>Browser (Safari)</td>
<td>United States (PA) (128.237.193.13)</td>
<td>10:37 am (1 hour ago)</td>
</tr>
<tr>
<td>Browser (Safari)</td>
<td>United States (PA) (128.237.193.13)</td>
<td>10:31 am (1 hour ago)</td>
</tr>
</tbody>
</table>

**Alert preference:** Show an alert for unusual activity. [change](#)

* indicates activity from the current session.

This computer is using IP address 128.237.193.13. (United States (PA))
Check Gmail Filtering & Forwarding

Carnegie Mellon University
Information Security Office
Check Gmail Filtering & Forwarding

The following filters are applied to all incoming mail:

Select: All, None

Create a new filter Import filters

The following email addresses are blocked. Messages from these addresses will appear in Spam:

You currently have no blocked addresses.

Select: All, None

Unblock selected addresses
It's easier than you think for someone to steal your password

Any of these common actions could put you at risk of having your password stolen:

- Using the same password on more than one site
- Downloading software from the Internet
- Clicking on links in email messages

2-Step Verification can help keep bad guys out, even if they have your password.
Thank you!