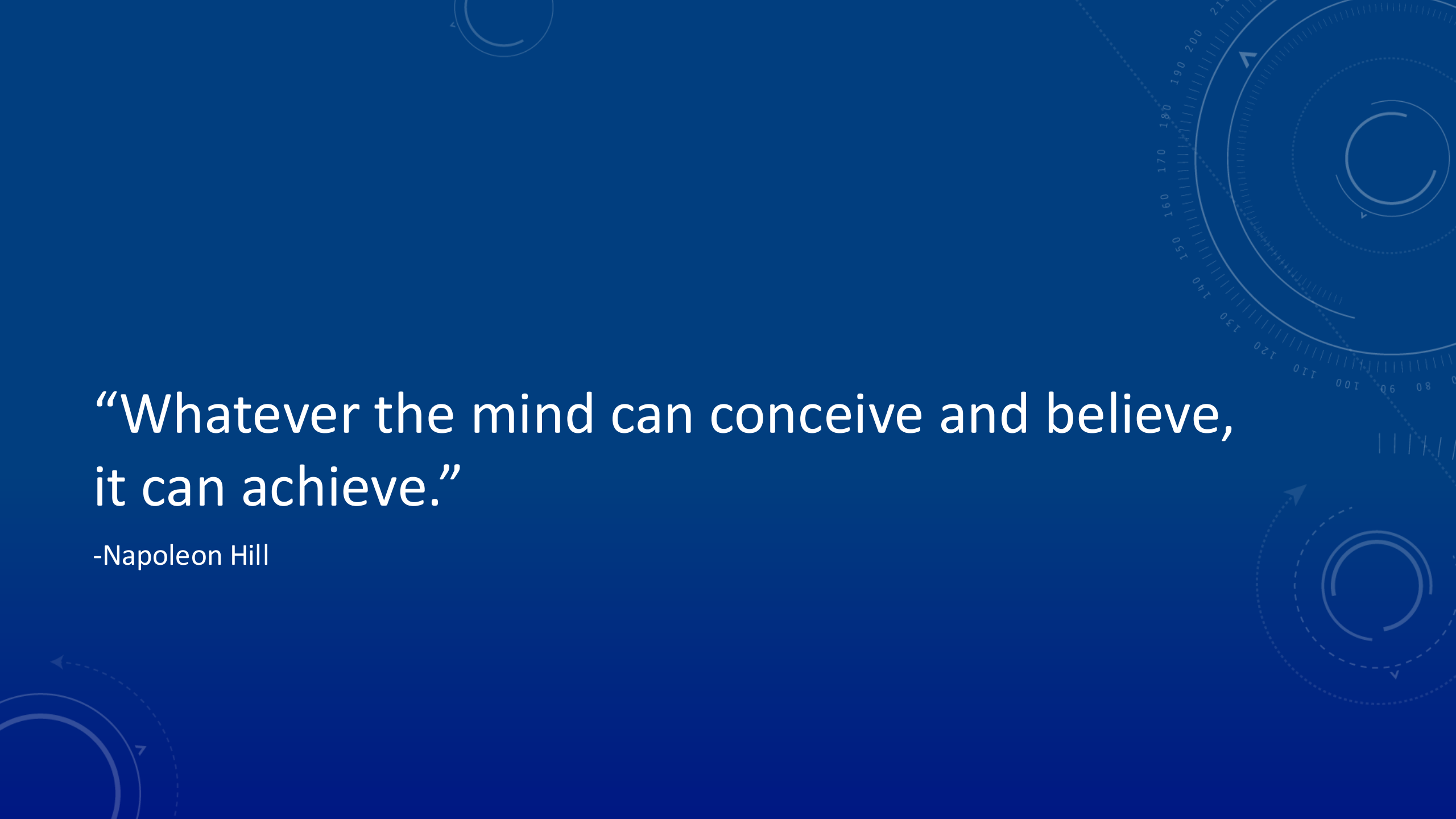


# PROMOTING A CULTURE OF INFORMATION SECURITY AT PACE UNIVERSITY

- Information security is everyone's responsibility. This session will explore the information security risks faced by the University and will explain each user's responsibilities and the best practices that will help to mitigate these risks. Passwords, safe web browsing, mobile security, social engineering attacks, malware, physical security, data handling, incident handling, roles and responsibilities, and promoting a culture of security will be some of the topics discussed.

CHRIS BOHLK, CISSP, C|EH  
PACE UNIVERSITY  
INFORMATION SECURITY OFFICER  
INFORMATION TECHNOLOGY SERVICES (ITS)  
235 ELM ROAD, WEST HALL 212A  
BRIARCLIFF MANOR, NY 10510  
(914)923-2649 OFFICE  
CBOHLK@PACE.EDU



“Whatever the mind can conceive and believe,  
it can achieve.”

-Napoleon Hill

# LEARNING OBJECTIVES

- To learn and understand information security principles and best practices that you are responsible to perform in order to help protect Pace's data.
- To understand that information security is everyone's responsibility. It is not just an IT problem.
- Take the knowledge that you learn today and immediately implement these habits into your daily work routine. Enthusiastically teach your colleagues and coworkers how to protect Pace's information assets to help promote a culture of information security awareness.





# YOU ARE A TARGET

**PACE**  
UNIVERSITY

Information Technology Services

## Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- Your bank or financial accounts, where they can steal or transfer your money.
- Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.
- Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.
- Your UPS or Fedex accounts, where they ship stolen goods in your name.

## Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- All the names, email addresses and phone numbers from your contact list.
- All of your personal or work email.

## Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- Your online gaming characters, gaming goods or gaming currencies.
- Any software licenses, operating system license keys, or gaming licenses.

## Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- Sending out spam to millions of people.
- Launching Denial of Service attacks.

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

[www.securingthehuman.org/ouch](http://www.securingthehuman.org/ouch)



## Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- Your Facebook, Twitter or LinkedIn account.
- Your email accounts.
- Your Skype or other IM accounts.

## Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- Hosting phishing websites to steal other people's usernames and passwords.
- Hosting attacking tools that will hack people's computers.
- Distributing child pornography, pirated videos or stolen music.

## Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- Your credit card information.
- Your tax records and past filings.
- Your financial investments and retirement plans.

## Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.
- Encrypting all the data on your computer and demanding payment to decrypt it.
- Tracking all websites you visit and threatening to publish them.

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at <http://krebsonsecurity.com>

# Universities Face a Rising Barrage of CyberAttacks

[NY Times Article on July 16, 2013](#)

# SECURITY THREATS

- Social Engineering
- External Hackers
- Disgruntled Employees
- Viruses
- Worms
- Trojans
- Keystroke Loggers
- Denial of Service (DOS)
- Phishing
- Identity Theft
- Data Leakage

# WHY DO WE CARE ABOUT SECURITY?

- Identity Theft
- Breach Disclosure Laws
- Financial Cost
- Legal Cost
- Time and money lost responding to a breach
- Loss of Reputation



# PERSONALLY IDENTIFIABLE INFORMATION (PII)

Some examples:

- Social security numbers
- Credit card numbers
- Bank account numbers
- Health information

# BEST PRACTICES

**PACE**  
UNIVERSITY

Information Technology Services

# PROTECT AGAINST SOCIAL ENGINEERING ATTACKS

- Be alert and vigilant

# EMAIL

- Delete suspicious email

Dear Webmail User,

Your mailbox has exceeded the allocated storage limit as set by the administrator, you may not be able to send or receive new mail until you upgrade your allocated quota.

To upgrade your quota, [CLICK HERE](#) to verify your email account.

Thank you for your anticipated cooperation.

System Administrator  
IT Helpdesk

To: Bohlk, Chris

Please view the document I uploaded for you using Google docs.

[Click here](#)

Just sign in with your email to view the document its very important.

Thank you



## Security Alerts:

Dear Citibank Customer,

All Citibank accounts access for online use are required to confirm their personal information due to a high volume of fraud and unauthorized access from outside US Territories.

For your protection your account is temporarily limited. An account that is temporarily limited is required to confirm the Account Information.

To successfully confirm your information we require your Citibank® Banking Card and Personal Identification Number (PIN) so you can access your accounts at ATMs and online. Here's how to confirm your account information online:

Go to [Citibank Online](#) page and complete the Card Verification form.

Agree to site Terms & Conditions and confirm your personal information.

You'll be successfully confirmed and your Citibank® Account is verified.

You may also want to view the Disclosures and Agreement that you agreed to when you applied, which you can do for the next 90 days at [Citibank Online](#).

Again, thank you for choosing Citibank.

**IMPORTANT:** Accounts are opened on Business Days only. If you apply on a Saturday, Sunday, or Bank Holiday or on a Business Day at a time when the processing of your application cannot be completed that same day, your account will be opened on the following Business Day. If this occurs, your account will receive the interest rate and annual percentage yield in effect on the date it is opened.

- Anticipate that you may receive fake UPS, Fedex, Amazon, or other emails trying to get you to click on links or provide personal information. Simply delete these emails.
- Also anticipate Holiday greetings, birthday messages, or gossip headlines as ways which attackers will try to steal your information or send you to a malicious website. Delete all such suspicious messages.

# WEB BROWSING

- Visit trusted web sites that are needed to conduct Pace University business.

## CAUTIOUSLY HANDLE PII

- You are responsible for safely handling PII in your possession.
- PII should only be stored on the designated servers and not copied to multiple locations or stored on local workstations, devices, USB drives, etc.
- PII may only be given authorization to authorized individuals with a 'need to know' to perform their job duties.
- You may not upload PII to public websites or any other publically accessible location.

# SOCIAL NETWORKS

- Do not upload PII to social to social networks.
- Be careful of what information you post to social networks

# PASSWORDS

- Never share your password with anyone
- Create a passphrase to help remember your password



## USE A PASSPHRASE

- A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."
- A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:
- "The\*?#>\*@TrafficOnTheIOI Was\* &#!#ThisMorning"
- All of the rules above that apply to passwords apply to passphrases.

# APPLY LATEST SECURITY PATCHES AND ENABLE ANTIVIRUS

- Keep your devices updated with the latest security updates
- Ensure antivirus is enabled with the latest definitions

# PHYSICAL SECURITY

- Keep track of and secure your devices

# PHYSICAL DATA DESTRUCTION

- Please contact the ITS Helpdesk at (914) 773-3333 for specific procedures

# LAPTOPS, USB DEVICES, AND MOBILE DEVICES

- PII (Personally Identifiable Information) should never be stored on laptops, USB Devices, and mobile devices

# YOUR HOME COMPUTER AND HOME NETWORK

- Secure your home computer and router with the latest patches and updates



# PUBLIC AND OTHER “UNTRUSTED” COMPUTERS

- Never logon with any of your Pace credentials from a public or “untrusted” computer, such as kiosks or Internet cafes.

# WI-FI SECURITY

- Use the Pace VPN (Virtual Private Network) to securely access resources if you are using WI-FI

# LAWS AND REGULATIONS

- FERPA - The Family Educational Rights and Privacy Act
- HIPAA - The Health Insurance Portability and Accountability Act
- GLBA- The Gramm-Leach Bliley Act
- SOX - Sarbanes-Oxley Act
- DMCA- The Digital Millennium Copyright Act
- PCI DSS - The Payment Card Industry Data Security Standards
- NYS Information Security Breach and Notification Act (Section 899-aa)

# INCIDENT REPORTING

- If you encounter or suspect an information security incident, immediately report this information to the Helpdesk at (914) 773-3333 ([pacehelpdesk@pace.edu](mailto:pacehelpdesk@pace.edu)). The Helpdesk should always be the initial point of contact. They will ensure that the event is documented and handed off to the appropriate party.

EVERYONE IS RESPONSIBLE FOR SECURITY

**PACE**  
UNIVERSITY

Information Technology Services

# CULTURE OF SECURITY

- You can help transform Pace University's information security culture



# INFORMATION SECURITY PROGRAM (ISP)

**PACE**  
UNIVERSITY

Information Technology Services

Review Pace's Information Security Policies to ensure that you know your responsibilities.

<https://www.pace.edu/its/about-its/it-policies>

Pace's Appropriate Use Policy

<https://www.pace.edu/its/about-its/it-policies/it-appropriate-use-policy>

Information Security at Pace University

<https://www.pace.edu/its/it-security>

SANS Security Newsletter

<http://www.securingthehuman.org/ouch>

SANS Tip of The Day

[https://www.sans.org/tip\\_of\\_the\\_day.php](https://www.sans.org/tip_of_the_day.php)

QUESTIONS?

