

Cybersecurity

College-Wide Learning Day, October 2004

An end-user-focused, non-technical introduction to information security

In other words...

*If you use any computer,
Here are the basics to do so
safely!*

Would you reply to this?

PLACE
STAMP
HERE

Valued AnyBank Customer,
The SEC requires AnyBank to conduct an annual audit. As part of this process, we are required to verify customer account information. Please complete the following and return this card as soon as possible.

Failure to reply may result in account suspension!

Name: _____

Social Security #: _____

Account #: _____

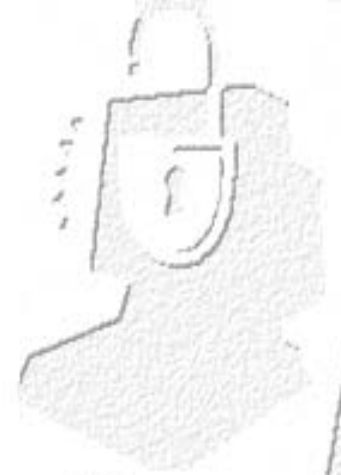
Expiration Date: _____

PIN or Password: _____

Thank you for your prompt response,
Internal Audit Team

AnyBank
Internal Audit Department
PO Box 623
Trenton, NJ 13579

What about...



From... Citi_security_services

To... Sinclair Citi Account Holders

Cc...

Subject: Urgent Fraud E-Lert - Action Required

Dear Citibank Customer,

At Citibank, we take security very seriously. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

At Citibank, we maintain your personal information and data according to strict standards of security and confidentiality as described in the Terms & Conditions that govern your use of this site. Online access to your account portfolio is only possible through a secure web browser.

In order to further protect your account, we have introduced new important security standards and browser requirements. Citibank security systems require that your computer system is compatible with our new standards.

This security update is effective immediately. Please [sign on](#) to Citibank Online in order to verify security update installation. Failure to do so may result in your account being compromised.



Back



Forward



Stop



Refresh



Home



Search



Favorites



Media



History

Address http://www.citibank.com

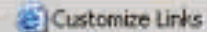


Go

Links



Yahoo!



Customize Links



Free Hotmail



Privacy • citi.com

Careers • Use Credit Wisely • Site Map • citicards.com • Español

Citi • Cards

Microsoft® Net
Learn More

Sign In

“Thank You”SMIntroducing ThankYou Redemptions Network,SM a new kind
of rewards program. Easy to earn, easy to redeem rewards.[Learn More](#)

... In the Spotlight ...

[Choose a Card / Apply](#)**Worry-free Protection**

- [Overview](#)
- [Security & You](#)
 - [Citi® Identity Theft Solutions](#)
 - [Safe Shopping](#)
 - [Virtual Account Numbers](#)
- [Privacy Policy](#)

Save Time and Money

- [Transfer Balances Now](#)
- [Learn More](#)
- [About Alerting Services](#)
- [Citi Cards with Rewards](#)

[Email Safety](#) **Secure Online Services**User ID [Sign-on](#)Password

- [Look Up User ID](#)
- [Forgot Password?](#)

[Register](#)• [About Online Services](#)

- [Manage your account](#)
- [Pay your bills](#)

- [Business Account Online Access](#)

• [Shop Smart & Safe Online](#)

Create a substitute card number in place of your real one, using Virtual Account Numbers.

• [ThankYou Redemptions NetworkSM](#)

A new rewards program that helps you redeem faster for the rewards you want! Start getting ThankYou Points today with the [Citi® Diamond Preferred® Rewards Card](#) or [CitiBusiness® Card with ThankYou NetworkSM](#).

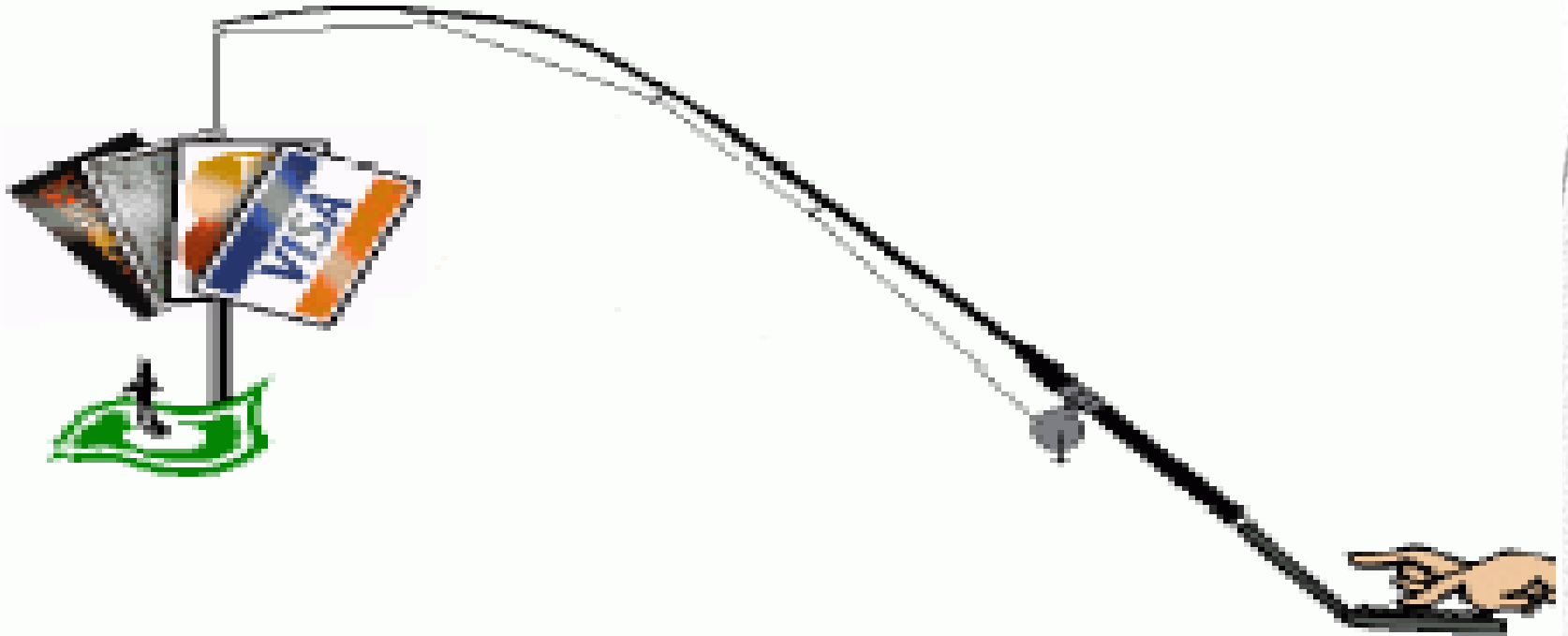
• [\\$5 Statement Credit](#)

Sign up for online statements & earn a \$5 credit!



Internet ms.ms.

Looks Genuine, **BUT...**



It's **PHISHING!**

Looks Genuine, **BUT...**

- Your **USER ID** and **PASSWORD** have been 'harvested'
- A 'Virus' or 'worm' may have infected your system
 - Zombie or Bot
 - Harvest more addresses
- A 'Trojan Horse' application that records and transmits every keystroke may be installed.



Identity Theft

**is the fastest growing crime in the
World**

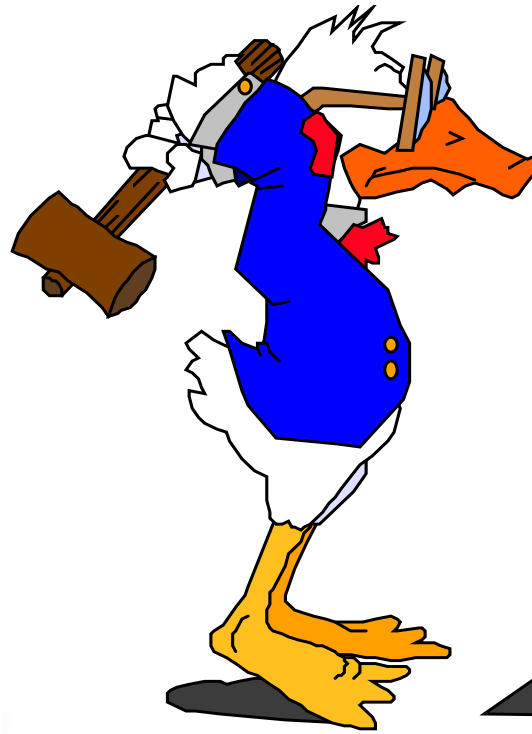
**In the U.S. alone, in 2003, it is
estimated over 10 million victims.**

Losses approach \$50 Billion.

(<http://www.ftc.gov/os/2003/09/synovatereport.pdf>)

ABSOLUTE EMAIL RULES

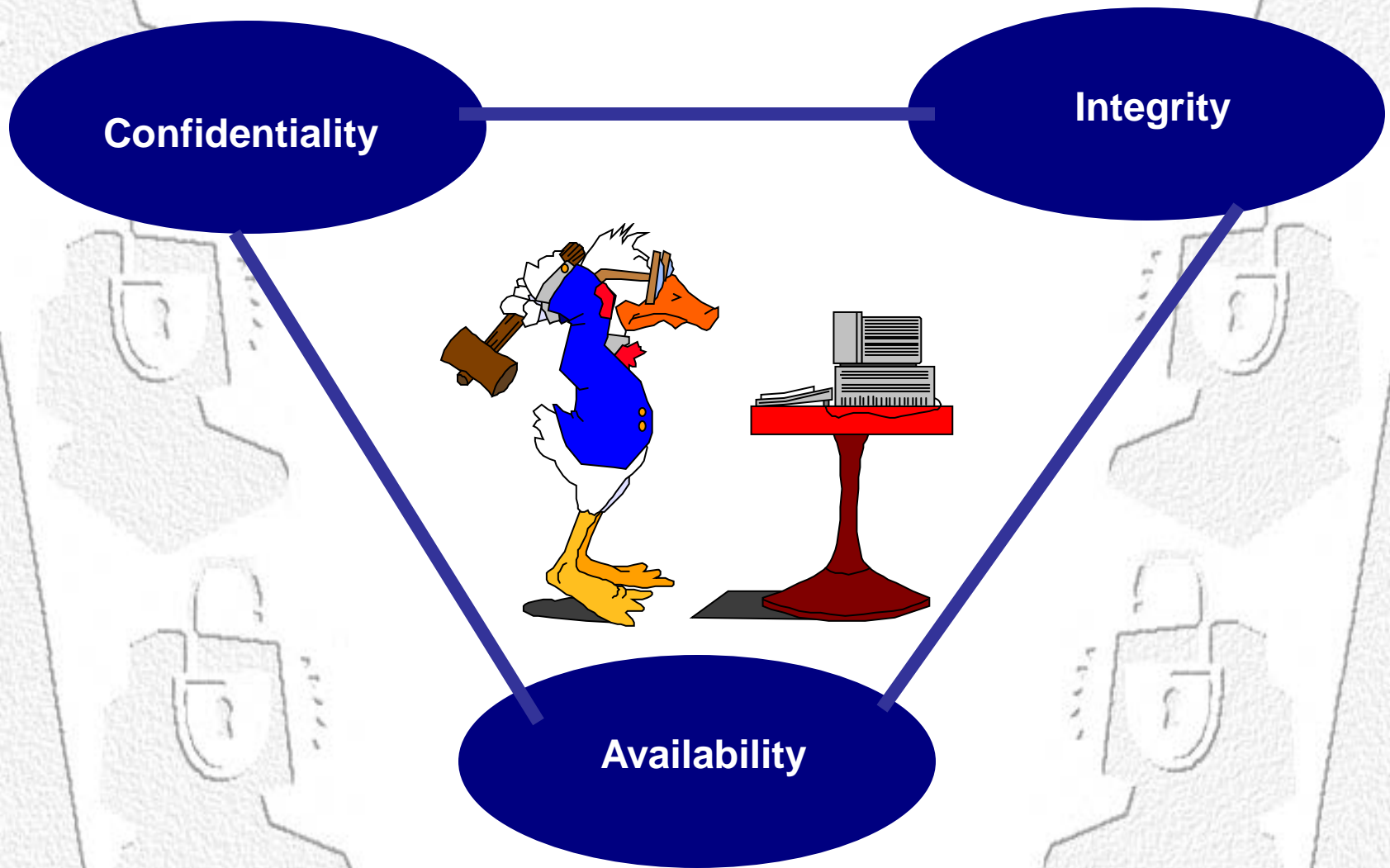
- **NEVER** send private or sensitive information via email
- **DO NOT** enter sensitive information or 'log-in' to a Web site you arrived on by clicking a hyperlink in an email message



What is

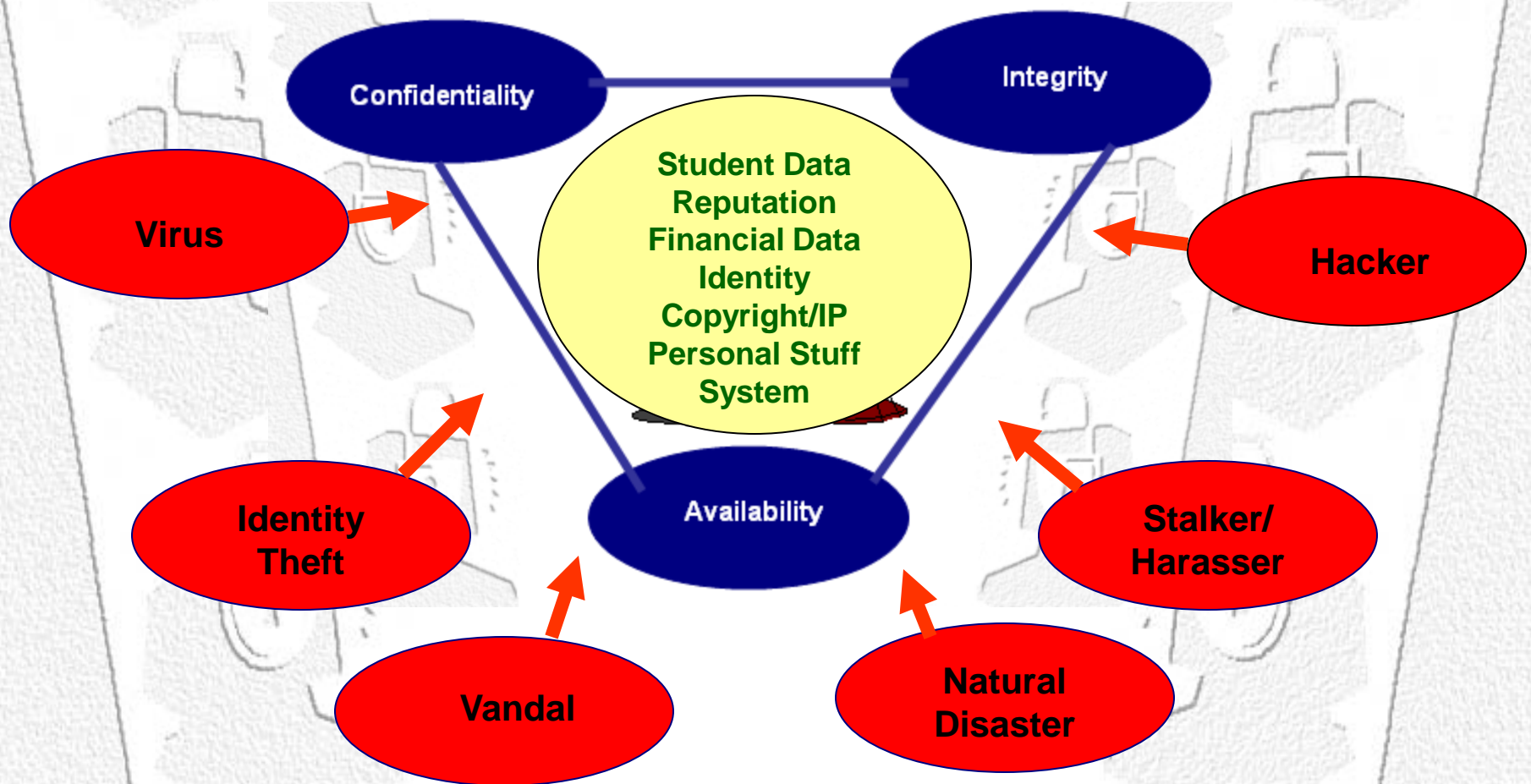
Cybersecurity?

“Official Definition”



“Practical Definition”

To decide whether information is “secure”, you must first decide what needs to be protected, next, identify the threats you care about, then, implement safeguards to mitigate the threats.



Some Perspective

- **There were an estimated 604.2 million people with internet access in 2002.**
- **All 604 million of them *can* communicate with your Internet connected computer.**
- **Any of the 604 million can ‘rattle the door’ to your computer to see if its locked.**

More Perspective

- To break into a safe, the safe cracker needs to know something about safes.
- To break into your computer, the computer cracker only needs to know *where to download* a program written by someone else who knows something about computers.



What Should We Do?

Email

Don't open email messages, attachments, or click on links in emails from unknown sources.

Be suspicious of any unexpected email attachments even if they appear to be from someone you know.

DON'T REPLY or otherwise acknowledge (such as a 'confirm receipt' message) that you have received a suspect message

Passwords

- **Use hard-to-guess passwords**
 - **At least eight characters long**
 - **Not found a common dictionary**
 - **Mix of:**
 - **upper case**
 - **lower case**
 - **numbers**
 - **special characters**

Passwords

- **Don't share your password**
 - If someone needs access, get them their own account, or (last resort) login yourself and 'shoulder-surf'
 - If posted on monitor, under keyboard, or in desk drawer – It's SHARED!
- **Change passwords regularly**
- **Don't use same password for 'routine access' as for sensitive information**

Passwords

- **If you suspect someone has guessed or otherwise knows your password:**
 - **Fix the ‘security lapse’ that revealed it**
 - **Change it to a new, hard-to-guess password**
- **If you suspect someone has accessed your account, report it.**

Back-up Your Data

- **Two Kinds of Computer Users**
 - Those who have already lost data
 - Those who are going to lose data in future
- **Back-up Options:**
 - “H” Drive
 - Network shares
 - CDs
 - “Zip” Drives, USB Drives

Back-up Your Data

- **Plan strategy based on risk**
 - Impact of loss
 - Sensitivity/Uniqueness
 - Cost/Time/Benefit to re-create
- **Keep original software CDs safe**
 - Make copies if possible

Beware of File Sharing

- **Unless you need it, TURN IT OFF**
- **Peer-to-Peer**
 - **Napster (the most infamous)**
 - **Kazaa**
 - **Grokster**
 - **Gnutella/Gnotella/Gnucleus**
- **SpyWare**
 - **Often 'bundled' with Freeware**

Turn It Off (when not in use)

- **Close Applications/Browser/Email**
- **Disconnect from the Internet (home)**
- **Shut-Down PC at end-of-day**

**This Protects YOU...
and OTHERS**

Virus Protection

- **Use & Update Anti-Virus software”**
 - Update regularly...**DAILY**
 - **SCC employees**
 - McAfee Antivirus free of charge
 - **Free AV tools available**
 - Trend Micro free on-line virus scanner
- **Schedule/Run ‘Full Scan’ regularly**

Firewalls

- **Work by filtering out and blocking unauthorized or potentially dangerous types of data from the Internet**
- **Windows XP, XP-SP2 built-in**
- **Free software firewalls are available**

Updates & 'Patches'

- **NO software is 100% secure**
 - Updates & Patches 'fix' known holes
- **Windows Users**
 - Run 'Windows Update' at least weekly
 - Me, 2000, XP users can 'auto update'
 - Install ALL **CRITICAL** updates

SpyWare

- Controversial, definition still 'fuzzy'

WORKING DEFINITION

- If software is collecting & reporting any information about my PC or use of my PC, and I don't know it's doing so--it's

Spyware!

SpyWare

- Some spyware harmless/marginally beneficial
- Illicit spyware is a threat...and a growing one
 - causes damage
 - steal personal information

Major A-V vendors now adding support to stop known backdoors & Trojan Horses

- Free spyware scanning software is available
- **BEWARE** - Some spyware advertises itself as anti-spy!



Why Should We Care?

Why Should We Care?

- **Be a responsible ‘cyber citizen’**
 - Even if you don’t think anything on your PC is worth protecting, how would you feel if your PC was used to hurt someone you care about?
- **Federal Laws Specifically Affecting HE**
 - **FERPA** (Family Educational Rights & Privacy Act)
 - **GLBA** (Gramm-Leach-Bliley Act)
 - **Patriot Act**

REMEMBER


A system, and the information accessed or stored by the system, is only as “secure” as the persons using the system make it.

Want a Catch-Phrase?

SEC-U-R-IT-Y

SECURITY – YOU ARE IT

Thanks to the University of Arizona, CCIT, for the Sec-UR-IT-y slogan!

The background features a repeating pattern of stylized, light-colored figures. Each figure is depicted from the waist up, wearing a suit and holding a rectangular sign in front of their chest. The figures are arranged in a grid-like pattern, with some appearing slightly more prominent than others. The overall style is simple and graphic.

Want More Information? Any Questions?

SCC InterOffice Mail—Address to:
Dan O'Callaghan
14-301

Voice: 512-2452

Email (**NOT SECURE!**): daniel.ocallaghan@sinclair.edu