Personal Cybersecurity

Think before you click!

Dan O’Callaghan

Sinclair Community College

SPDD, Dec 19, 2012

What is Information Security?

- CIA
  - Confidentiality
    - PII Exposure
    - Fraud/ID theft
    - ?Privacy?
  - Integrity
    - Deletion
    - Changing
  - Availability
    - Deletion
    - Lockout
    - Email blocking

Basic Attack Definitions

- Malware – Virus, Worm, Trojan
  - Virus spreads via user interaction
  - Worm typically does NOT require direct user action
  - Trojan (Horse)
    - Appears to offer desirable function (and may)
    - Actually (or also) contain malicious payload
      - ROGUE AV, Extortionware
- Back Doors/Persistent Threats
  - Secret access to PC or account (pwned)
  - Often installed as Trojan payload

Basic Attack Definitions

- Social Engineering
  - ‘Con’ user to compromise
- Botnets
  - Networks of compromised PCs under remote control
  - 100’s, 1000’s, 10,000’s ???
  - Used for multiple illicit purposes
    - Sending spam
    - Phish host/receive
    - Illicit file server (child porn)
    - DDOS

Why should YOU care?

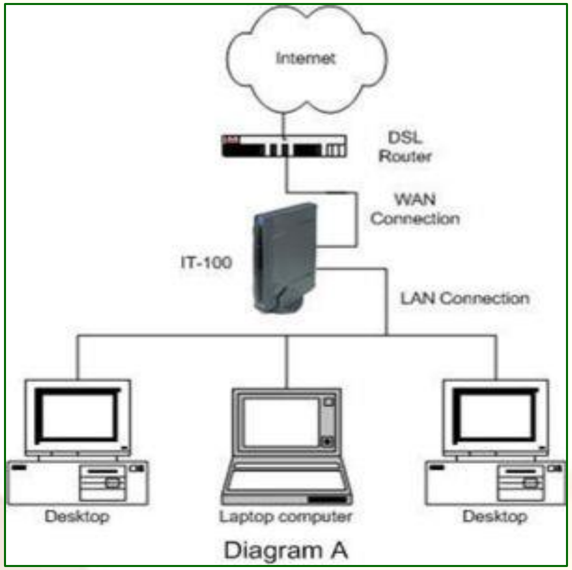
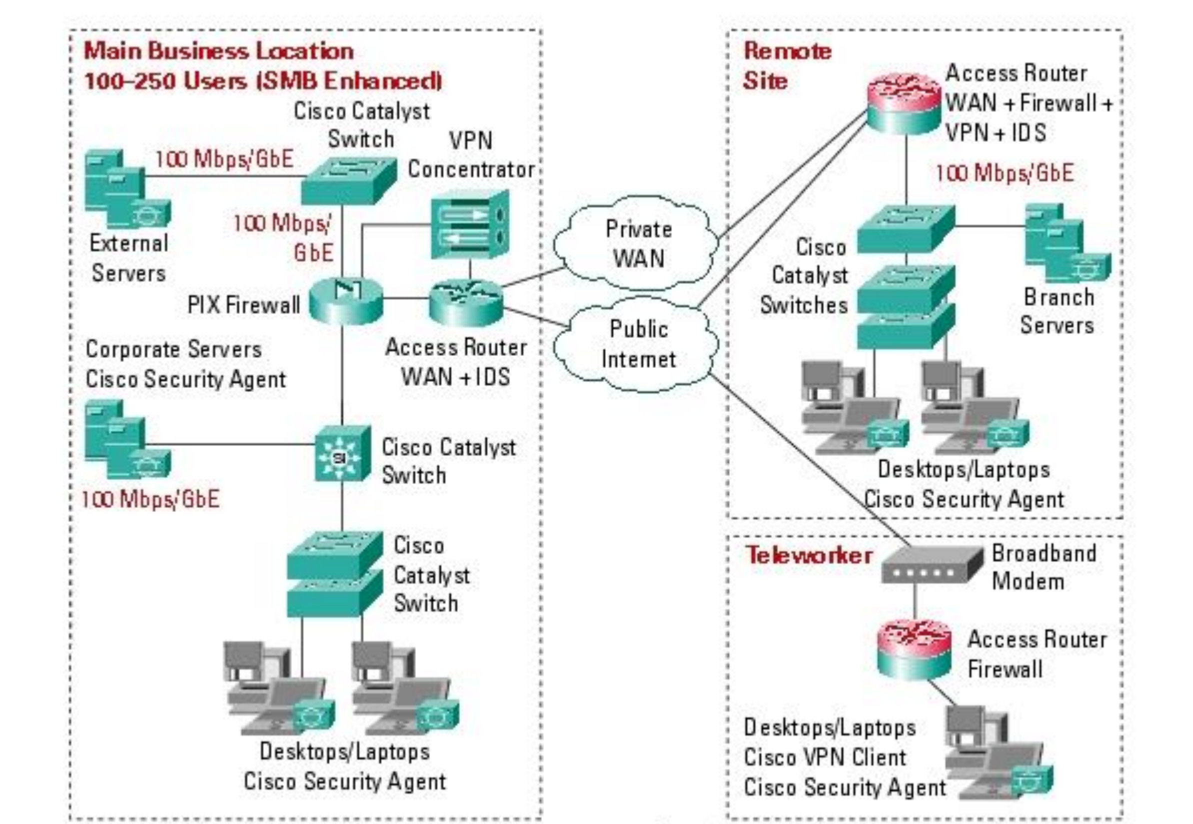
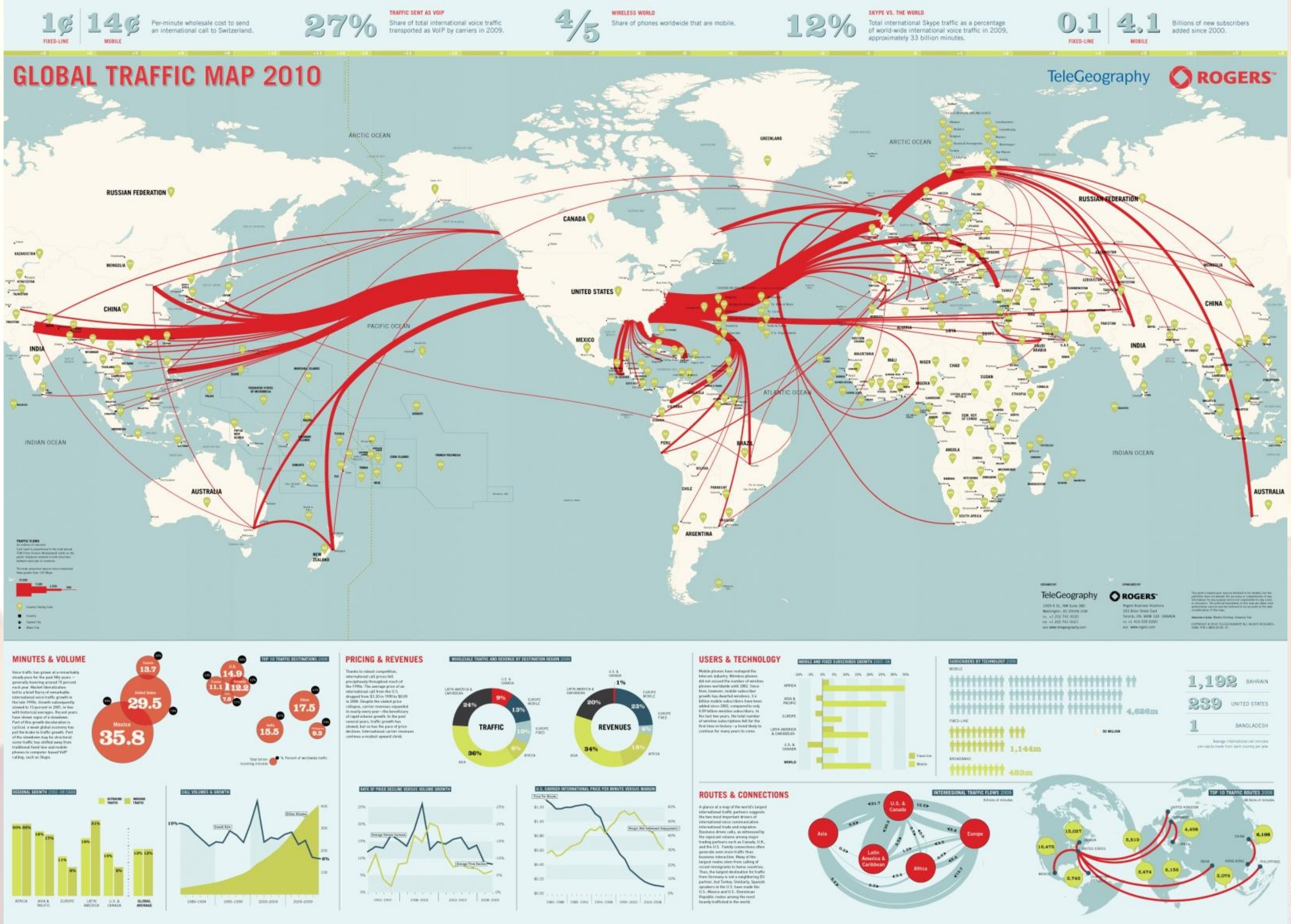


Diagram A



This network blueprint is intended to be an educational resource and a starting point in planning your network solution; it is not a final recommendation from Cisco. To determine the deployment at appropriate for your company we suggest you work with a Cisco representative, Cisco channel partner, or a solutions provider.

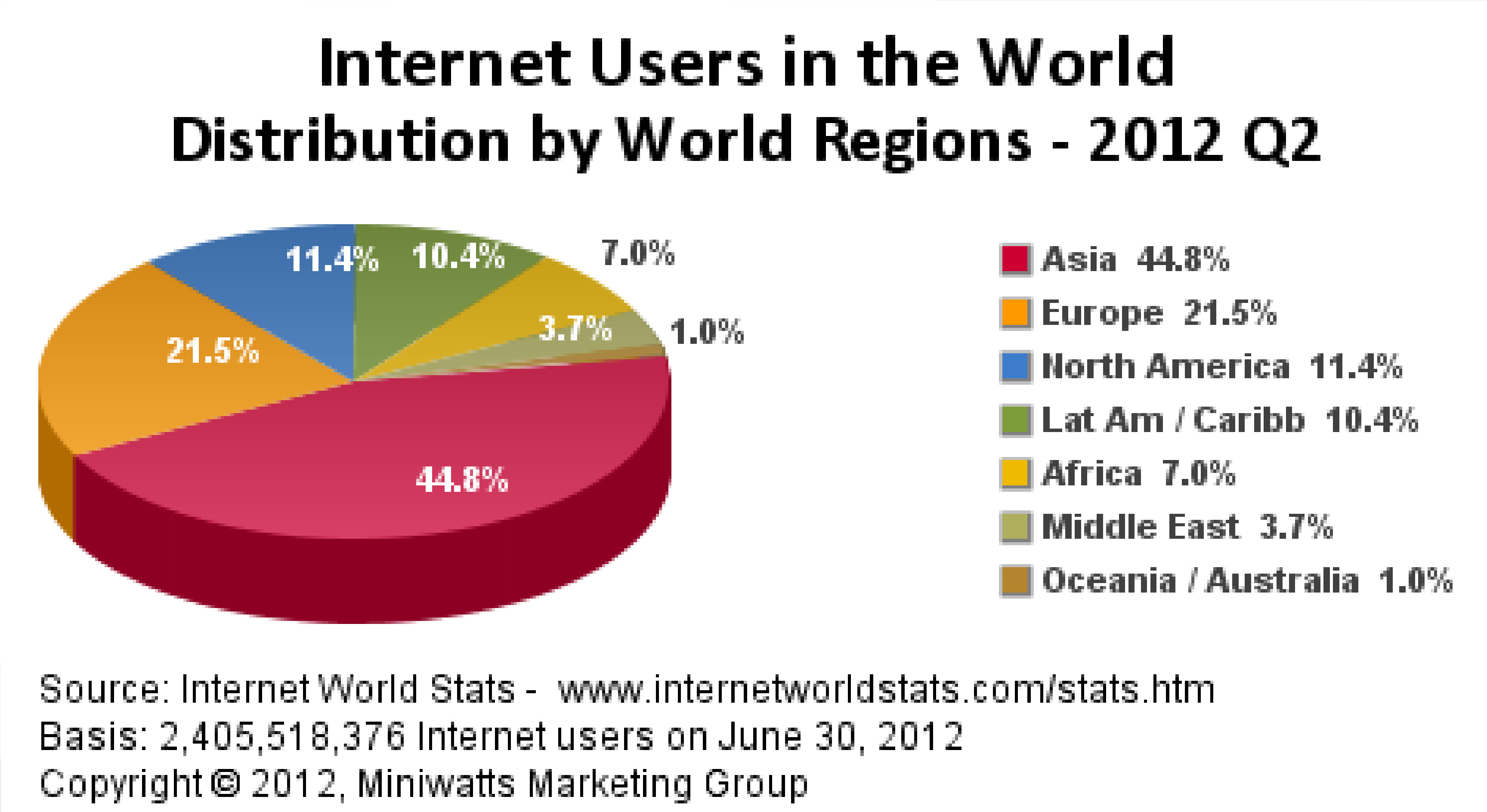
Why should YOU care?



By the numbers…

- 7+B – Global population (census.gov)
- 2.4+B – Global Internet users (internetworldstats.com)
- 34.3% - Global Internet penetration rate (internetworldstats.com)
- ~6B – Global mobile phones subscribers (itu.org)
  - 1B+ are ‘smart’
- 314+M – US population (census.gov)
- 245+M – US Internet users (internetworldstats.com)
- 78.1% - US Internet penetration rate (internetworldstats.com)
- ~322M US mobile phone subscribers (ctia.org)
  - 101% saturation, nearly 50% ‘smart’

By the numbers…



Internet Users in the World
Distribution by World Regions - 2012 Q2

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 2,405,518,376 Internet users on June 30, 2012
Copyright © 2012, Miniwatts Marketing Group

By the numbers…

World Facebook – 1 billion users

10/4/2012 http://news.cnet.com/8301-1023_3-57525797-93/facebook-hits-1-billion-active-user-milestone/

USA Facebook- 166,029,240

9/30/12, 52.9% penetration rate

Current Threat - Attackers

Early (Hollywood) Profile	Mature Profile
1980's ~ 2003	(~2003 – present)
•Male	•Male
•Age 14-24	•More experienced, older
•Computer/Tech Obsessed	•Highly skilled and extensive tech knowledge
•No 'real' social life, much idle time	•On-line social life, increasingly organized (state sponsored?)
•Target: Usually Infrastructure Widespread, random, 'opportunity'	•Target: Data, Infrastructure/resources 'targeted' to goal/need
•Motivation: Curiosity, Ego	•Motivation: Access, Information, stealthy persistence PROFIT!

Current Threat - Attackers

What are they after?

- Data useful for commercial advantage or committing fraud, (particularly personal and financial data)
- Connectivity & resources provided by the system – Botnets

How do they get it?

- Low-profile tools, targeted and too small to trigger the Security vendors' radar
- Attack data-rich and profitable targets
- **Exploit weakest link - USERS**

Current Threat - Users

Typical User Profile?

- ALL users have:
  - Some level of “authorized access”
  - Some level of “authorized use”
  - Some method --usually userid/password– that provides identification/authentication to the “authorized” resources
- Excess Capacity

Primary Attack Methods

- Deception – Email, Text, IM, Social Media
  - Social engineering- convince user to compromise account or machine
  - Scams/Fraud **PHISHING!**
  - Many include a malware persistent component
- E-Mail
  - Attachments
  - Content…particularly links, also embedded malware
- Web
  - Active content
  - Ads
  - “Drive-By”

Defense?
(Technical Practices)

Basic “Technical” Security

(keep a clean machine)

- Firewall ON (http://www.youtube.com/watch?v=33Yuryw2uhM)
- Anti-Malware software ON & auto-update
  - Schedule routine scans
- Microsoft & other software auto-update
  - Do not ignore non MS updates
- DO NOT use an “Admin” account for routine PC use
  - Anything YOU can do, your browser can do
- Protect ALL your devices (if possible)

Defense?
(Effective Practices)

1. Protect Your Information

- **Secure your financial/sensitive accounts:**
  - Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- **Develop good password practices**

  http://www.youtube.com/watch?v=1QptFg8VQ88
  - Passwords should:

    be at least eight characters

    include uppercase, lowercase letters, numerals and symbols

    be secret – if someone else knows it, it is not!
- **Unique account = unique password**
  - Separate passwords for every account, especially sensitive ones

1. Protect Your Information

- **Write it down and keep it safe::**
  - Everyone can forget a password. Keep a list that’s stored in a safe, secure place away from your computer.
  - Consider password manager (lastpass, keypass)
- **Own your online presence**
  - When available, set the privacy and security settings on websites to your comfort level for information sharing.
  - It’s OK to limit who you share information with.
- **Back it up**
  - Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

2. Think Before You Click

- **When in doubt, throw it out!**
  - Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
- **Know where/how you connect**
  - Public Wi-Fi hotspots: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your device.
- **Protect your $$$**
  - When banking/shopping, check for site security. Look for web addresses with "https://" or "shttp://"
    "Http://" is not secure.

3. Be “Web Wise”

- **Stay current. Keep pace with new ways to stay safe online:**
  - Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- **Think before you act:**
  - Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.

4. Be “a Good Online Citizen”

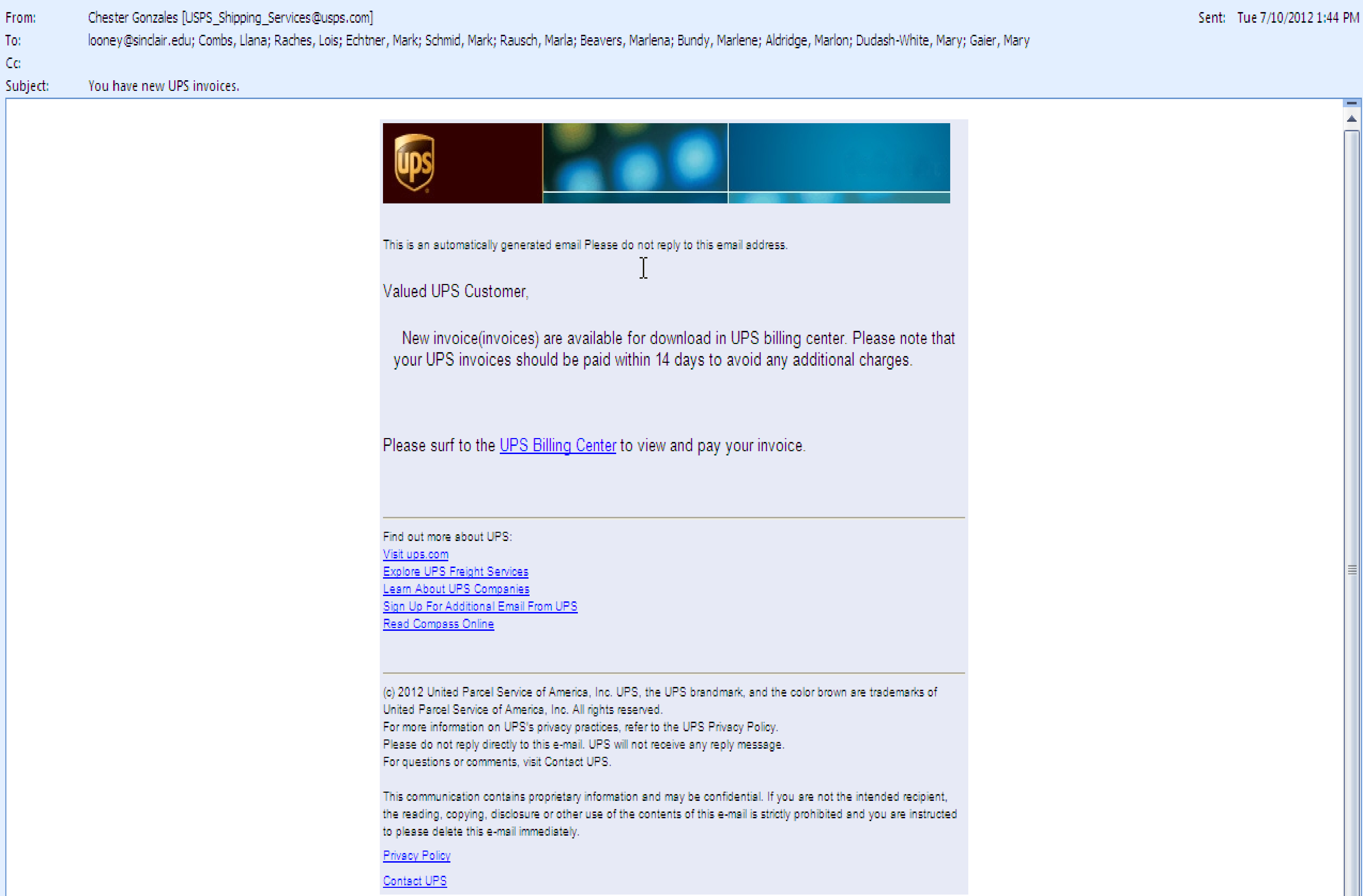
- **Safer for me more secure for all:**
  - What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- **Post only about others as you have them post about you**
- **Help fight cyber crime:**
  - Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center (www.ic3.gov) and to your local law enforcement or state attorney general as appropriate.

5. Dispose of Information Properly

- – Before discarding your computer or portable storage devices, you need to be sure that the data contained on the device has been erased or "wiped." Read/writable media (including your hard drive) should be "wiped" using Department of Defense (DOD) compliant software.
- – Recycle home PCs, but be aware much of this is contracted overseas

- http://eraser.heidi.ie/

Examples of Common Attacks



From: Chester Gonzales [USPS_Shipping_Services@usps.com]

Sent: Tue 7/10/2012 1:44 PM

To: looney@sinclair.edu; Combs, Llana; Raches, Lois; Echtner, Mark; Schmid, Mark; Rausch, Marla; Beavers, Marlena; Bundy, Marlene; Aldridge, Marlon; Dudash-White, Mary; Gaier, Mary

Cc:

Subject: You have new UPS invoices.

This is an automatically generated email Please do not reply to this email address.

Valued UPS Customer,

New invoice(invoices) are available for download in UPS billing center. Please note that your UPS invoices should be paid within 14 days to avoid any additional charges.

Please surf to the UPS Billing Center to view and pay your invoice.

Find out more about UPS:
Visit ups.com
Explore UPS Freight Services
Learn About UPS Companies
Sign Up For Additional Email From UPS
Read Compass Online

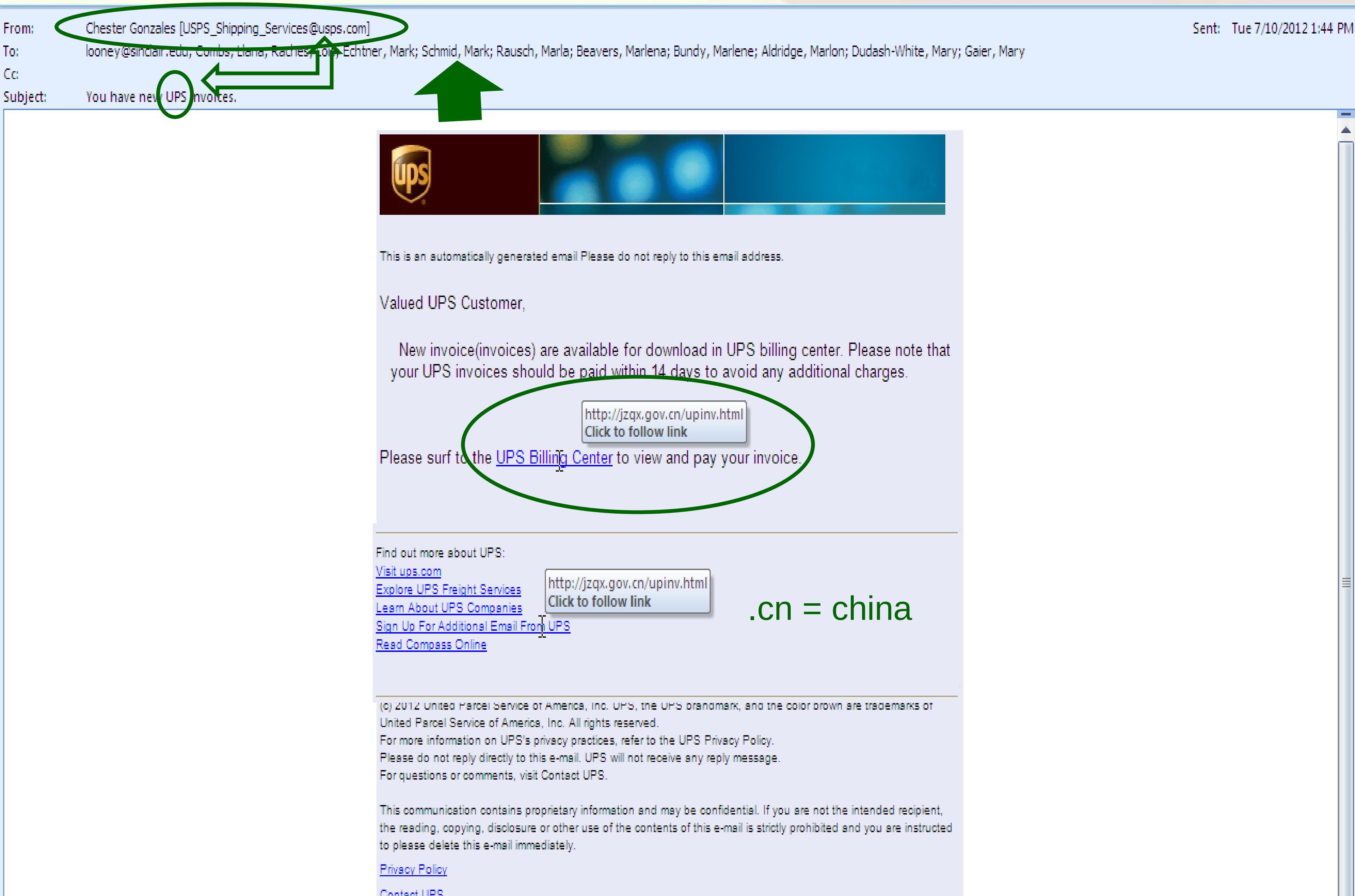
(c) 2012 United Parcel Service of America, Inc. UPS, the UPS brandmark, and the color brown are trademarks of United Parcel Service of America, Inc. All rights reserved.
For more information on UPS's privacy practices, refer to the UPS Privacy Policy.
Please do not reply directly to this e-mail. UPS will not receive any reply message.
For questions or comments, visit Contact UPS.

This communication contains proprietary information and may be confidential. If you are not the intended recipient, the reading, copying, disclosure or other use of the contents of this e-mail is strictly prohibited and you are instructed to please delete this e-mail immediately.

Privacy Policy

Contact UPS

Examples of Common Attacks



From: Chester Gonzales [USPS_Shipping_Services@usps.com]

Sent: Tue 7/10/2012 1:44 PM

To: looney@sinclair.edu; Combs, Llana; Raches, Lori; Echtner, Mark; Schmid, Mark; Rausch, Marla; Beavers, Marlena; Bundy, Marlene; Aldridge, Marlon; Dudash-White, Mary; Gaier, Mary

Cc:

Subject: You have new UPS invoices.

This is an automatically generated email Please do not reply to this email address.

Valued UPS Customer,

New invoice(invoices) are available for download in UPS billing center. Please note that your UPS invoices should be paid within 14 days to avoid any additional charges.

http://jzqx.gov.cn/upinv.html
Click to follow link

Please surf to the UPS Billing Center to view and pay your invoice.

Find out more about UPS:

Visit ups.com
Explore UPS Freight Services
Learn About UPS Companies
Sign Up For Additional Email From UPS
Read Compass Online

http://jzqx.gov.cn/upinv.html
Click to follow link

.cn = china

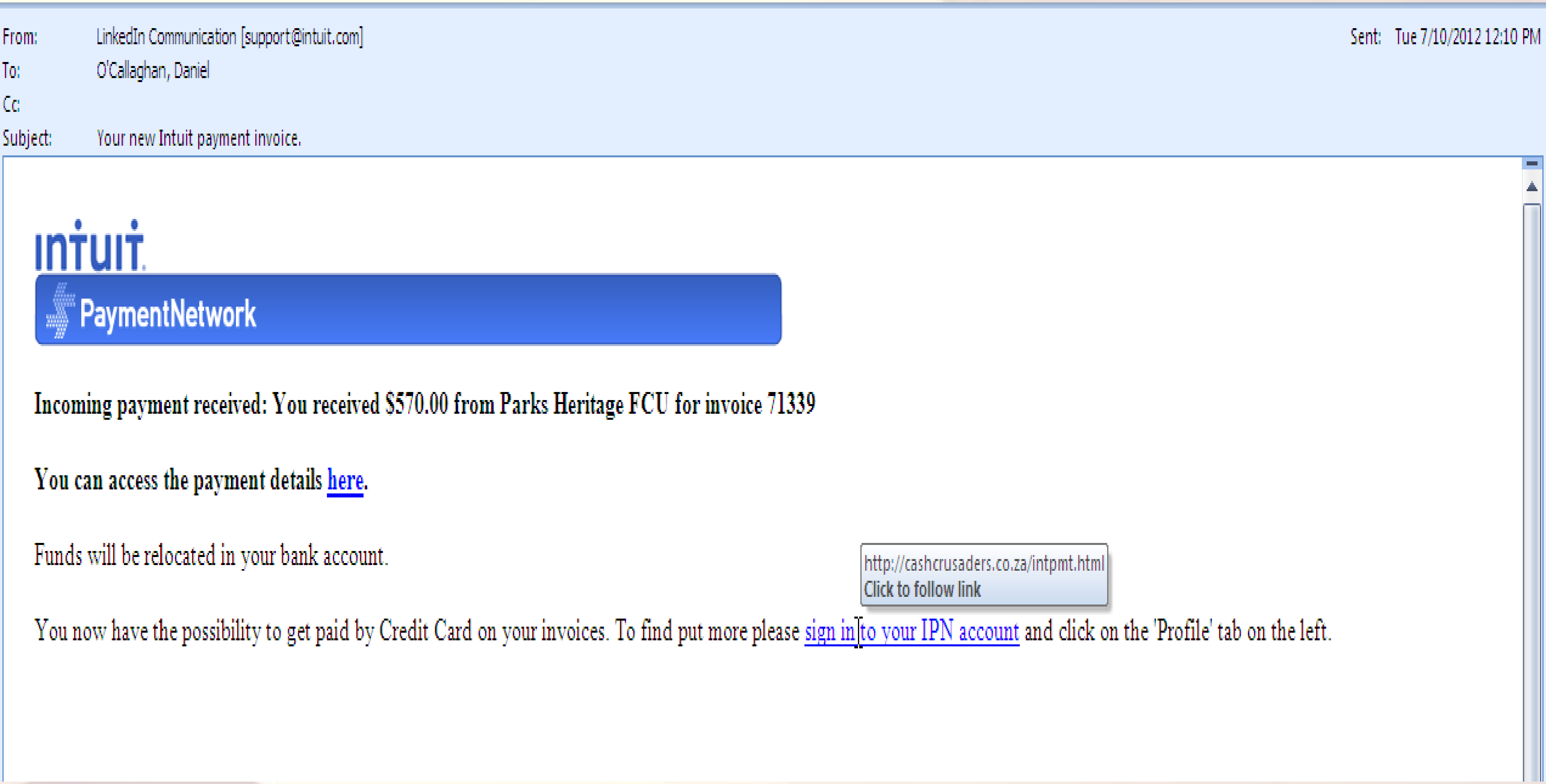
(c) 2012 United Parcel Service of America, Inc. UPS, the UPS brandmark, and the color brown are trademarks of United Parcel Service of America, Inc. All rights reserved.
For more information on UPS's privacy practices, refer to the UPS Privacy Policy.
Please do not reply directly to this e-mail. UPS will not receive any reply message.
For questions or comments, visit Contact UPS.

This communication contains proprietary information and may be confidential. If you are not the intended recipient, the reading, copying, disclosure or other use of the contents of this e-mail is strictly prohibited and you are instructed to please delete this e-mail immediately.

Privacy Policy

Contact UPS

Examples of Common Attacks



From: LinkedIn Communication [support@intuit.com]

Sent: Tue 7/10/2012 12:10 PM

To: O'Callaghan, Daniel

Cc:

Subject: Your new Intuit payment invoice.

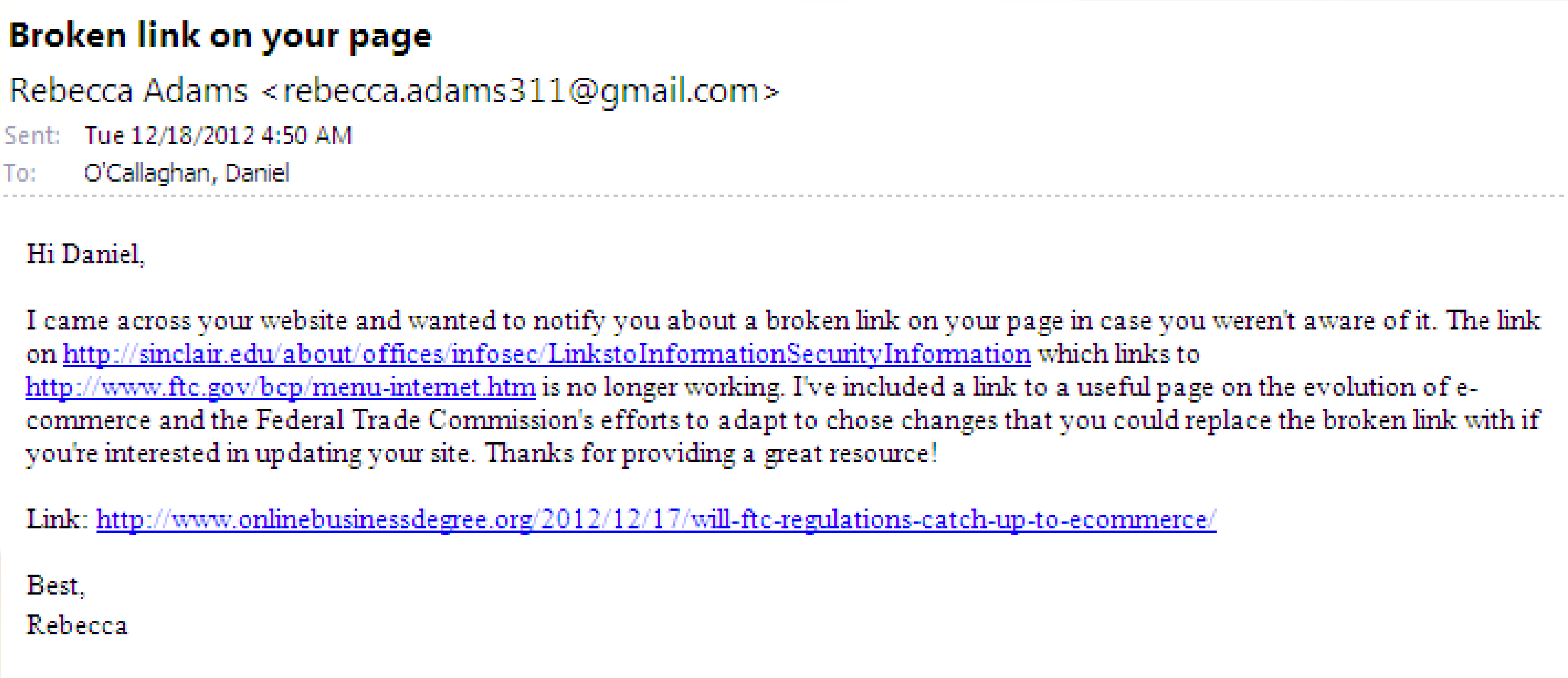
Incoming payment received: You received $570.00 from Parks Heritage FCU for invoice 71339

You can access the payment details here.

Funds will be relocated in your bank account.

You now have the possibility to get paid by Credit Card on your invoices. To find put more please sign in to your IPN account and click on the 'Profile' tab on the left.

Examples of Common Attacks



Broken link on your page

Rebecca Adams <rebecca.adams311@gmail.com>

Sent: Tue 12/18/2012 4:50 AM

To: O'Callaghan, Daniel

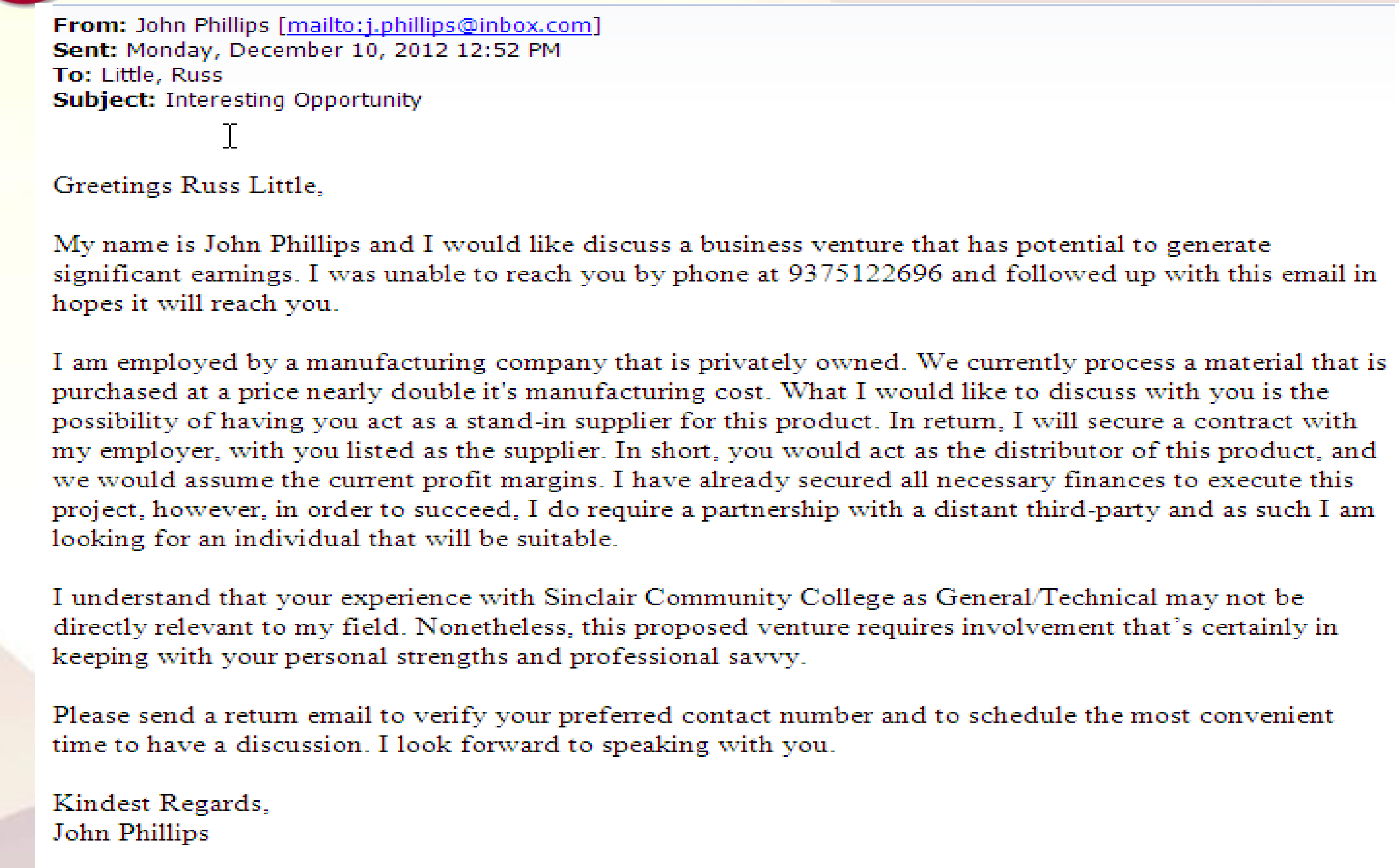
Hi Daniel,

I came across your website and wanted to notify you about a broken link on your page in case you weren't aware of it. The link on http://sinclair.edu/about/offices/infosec/LinkstoInformationSecurityInformation which links to http://www.ftc.gov/bcp/menu-internet.htm is no longer working. I've included a link to a useful page on the evolution of e-commerce and the Federal Trade Commission's efforts to adapt to chose changes that you could replace the broken link with if you're interested in updating your site. Thanks for providing a great resource!

Link: http://www.onlinebusinessdegree.org/2012/12/17/will-ftc-regulations-catch-up-to-ecommerce/

Best,
Rebecca

Examples of Common Attacks



From: John Phillips [mailto:j.phillips@inbox.com]
Sent: Monday, December 10, 2012 12:52 PM
To: Little, Russ
Subject: Interesting Opportunity

Greetings Russ Little,

My name is John Phillips and I would like discuss a business venture that has potential to generate significant earnings. I was unable to reach you by phone at 9375122696 and followed up with this email in hopes it will reach you.

I am employed by a manufacturing company that is privately owned. We currently process a material that is purchased at a price nearly double it's manufacturing cost. What I would like to discuss with you is the possibility of having you act as a stand-in supplier for this product. In return, I will secure a contract with my employer, with you listed as the supplier. In short, you would act as the distributor of this product, and we would assume the current profit margins. I have already secured all necessary finances to execute this project, however, in order to succeed, I do require a partnership with a distant third-party and as such I am looking for an individual that will be suitable.

I understand that your experience with Sinclair Community College as General/Technical may not be directly relevant to my field. Nonetheless, this proposed venture requires involvement that's certainly in keeping with your personal strengths and professional savvy.

Please send a return email to verify your preferred contact number and to schedule the most convenient time to have a discussion. I look forward to speaking with you.

Kindest Regards,
John Phillips

Sinclair Community College

More Information?
Any Questions?

Dan O'Callaghan
Sinclair Community College
444 W Third St, 13-000B
Dayton, OH 45402

Voice: 512-2452
Email (NOT SECURE!): daniel.ocallaghan@sinclair.edu

Information Security