1. WHO ARE YOU & 2. WHY SHOULD WE LISTEN?

1. Quinn Shamblin
   - Executive Director & Information Security Officer
   - Digital Forensics Professional
   - CISSP, GCFA, PMP
   - qrs@uc.edu
   - 358-6310

2. …Because it's interesting stuff & while you probably know some of it, you probably will still learn something. (Plus, I have a few good stories…)
MALWARE AND PHISHING ARE CHANGING TACTICS

(Starting with some stuff you probably know, but just making sure…)

• Email
  • 419
    • Spear-phishing e-mails specifically targeted to you
• Web Sites – Clones, forwarders, ads, drive-by download
• Social Networking Websites
• IM

WILL YOU KNOW AN EMAIL SCAM WHEN U C IT?

• Standard Tricks
  • Bad English language usage or syntax
  • Misspellings (in messages from “major companies”)
  • Things from companies you don’t do business with
• Better Tricks
  • ANYTHING about passwords or money
  • Know the common scams (top ten list)
    http://netforbeginners.about.com/od/scamsandidentitytheft/ss/top10inetscams.htm
  • Hover check
UPDATE YOUR ONLINE BANKING INFORMATION

Dear Bank Of America Customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:
1. A recent change in your personal information (i.e. change of address).
2. Submitting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by clicking the link below:


If your account information is not updated within 48 hours then your ability to access your account will become restricted.

Thank you

The Bank of America Accounts Management Department

---

THIS CREDIT CARD TRANSACTION WILL APPEAR ON YOUR BILL AS "PAYPAL INPHONIC***"

This email confirms that you have paid INPHONIC (sales@inphonic.com) $239.95 USD using PayPal. This credit card transaction will appear on your bill as "PAYPAL INPHONIC***".

PayPal Shopping Cart Contents

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Quantity</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW MOTOROLA V3 PINK RAZR RAZOR QUAD-BAND CELL PHONE</td>
<td>1</td>
<td>$219.95 USD</td>
</tr>
</tbody>
</table>

Cart Subtotal: $219.95 USD
Shipping Charge: $20.00 USD
Cart Total: $239.95 USD

Shipping Information

Shipping Info: Richard McCoy
102 N Magnolia Tr.
Waco, MS 04172
United States

Address Status: Unconfirmed

If you haven’t authorized this charge, click the link below to cancel the payment and get a full refund.

Dispute Transaction ► http://intergate.gunterisd.org/~guest/index.html

Thank you for using PayPal
The PayPal Team
Dear Fifth Third bank business/commercial customer,


Fifth Third Protection Department apologizes for the inconveniences caused to you, and is very grateful for your cooperation.

To start the confirmation procedure, click the following link:

http://www.53.com/bank/ing portal/session/1bcconfirm

Copyright © 2005 Fifth Third Bank. Member FDIC. Equal Housing Lender. All Rights Reserved

---

From: IRS [mailto:service-tellers.gov]
Sent: Friday, February 23, 2007 3:57 PM
Subject: IRS Service: Refund your card with $63.80
Importance: High

Internal Revenue Service
United States Department of the Treasury

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $63.80. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here

JOB POSTINGS

Hello,

I am representing Company SPB Stream, which is looking for full-time/part-time financial contractors.

SPB Stream is an international trading company and we are looking for employees that are eligible to work with financial correspondence.

Requirements:
- basic computer knowledge,
- approximately 2 hours per day,
- good communication skills,
- bank account to withdraw/receive funds.

Money turnover of our company has already reached certain amounts and we are looking for regional managers, who are able to manage customers database.

Salary is based on the contract and depends on amount of work. Usually it is about $35000 per year, except for taxes. This is a part-time job and you will need to prove correspondence in order to qualify for higher rates and full-time job status.

As regional employee you will have good perspective to increasing workload and salary in accordance with your efforts.

Please visit www.spbstream.com for more details.

AVOID PHISHING AND MALWARE

- DON'T CLICK LINKS in emails
  - Type the site name (one you know) into your browser directly
- Never send sensitive account information in e-mail (Account numbers, SSN, passwords)
- Never give any password out to anyone
- Avoid dodgy web sites
- Pay attention to certificates and phishing filters
- More tips later…
THE HATTER’S WONDERLAND

- Keylogging
- Clipboard Theft
- Drive-by downloads
- XSS/XSRF
- BeEF: Browser Exploitation Framework
- Metsploit
- Much more

WIRELESS ACCESS POINTS VIA PHONE

- KNOW who you are connecting too
  - Ask for SSID
- Mobile wireless access points
- SSL Strip
SPEAKING OF SMARTPHONES

- Phone locking - PIN / PW / Pattern
- Browser Form / PW saving
- Anti-virus - https://www.mylookout.com
- Marketplace
  - Smobile: “about 20 percent of the 48,000 apps in the Android marketplace allow a third-party application access to sensitive or private information”…“some of the apps were found to have the ability to do things like make calls and send text messages without requiring interaction from the mobile user.”
- Jail breaking
- Secure your cellphone, step-by-step

SOCIAL NETWORKING SITES

- Very cool info/life sharing, but there are things to think about…
  - pleaserobme.com
  - Password reset security questions
- Facebook security tips
DEBUNKING THE NO-MALWARE MYTH FOR MACS

• Serious crimeware developers simply hadn't bothered with the Mac until few years ago, the audience was too limited to be worth the effort. But they are now.

• Macs (due largely to Safari) have been the first to fall in pwn2own 2007, 2008, 2009, 2010
  http://en.wikipedia.org/wiki/Pwn2Own

• GET ANTIVIRUS
  Free from BU at

USB = ULTIMATE SECURITY BACKDOOR

• The 30 second thief
  • Data Extraction, Key logging, Malware, C&C
  • Persistent, Self Propagation
LEARN SECURE CODING PRACTICES

SQL INJECTION

- Compromises database query code

```
select from table "users" where user='%user%' and pw='%pass%'
```

- Login without knowing a user name or password
  user: `or 1=1--`
  admin: `or 1=1--`
THE KEYS TO THE KINGDOM

PASSWORD CRACKING

- Password crackers can try passwords at a rate of over 100,000 each second

<table>
<thead>
<tr>
<th>Password length /charset</th>
<th>26 (no case, letters only)</th>
<th>36 (no case, letters &amp; digits)</th>
<th>52 (case sensitive)</th>
<th>96 (all printable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1 min</td>
<td>13 min</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>10 min</td>
<td>1 hr</td>
<td>22 hr</td>
</tr>
<tr>
<td>6</td>
<td>50 minutes</td>
<td>6 hrs</td>
<td>2.2 days</td>
<td>3 months</td>
</tr>
<tr>
<td>7</td>
<td>22 hrs</td>
<td>9 days</td>
<td>4 months</td>
<td>23 yrs</td>
</tr>
<tr>
<td>8</td>
<td>24 days</td>
<td>10.5 months</td>
<td>17 yrs</td>
<td>2,287 yrs</td>
</tr>
<tr>
<td>9</td>
<td>21 months</td>
<td>32.6 yrs</td>
<td>881 yrs</td>
<td>219,000 yrs</td>
</tr>
<tr>
<td>10</td>
<td>45 yrs</td>
<td>1,199 yrs</td>
<td>45,838 yrs</td>
<td>21 million yrs</td>
</tr>
</tbody>
</table>
PASS WORD SAVING | AUTO-LOGIN

• Useful, but with a major downfall
• If your computer is compromised, *everything* you connect to is compromised
• If you get owned, everything on your computer is owned
• Password auto-storage / Password wallets

YOU MIGHT UNDERESTIMATE THE SNEAKY
Why should I CARE?
HOW DOES IDENTITY THEFT HAPPEN?

- Identity thieves may:
  - Go through your trash or “dumpster dive”
  - Steal your wallet or purse
  - Steal your mail or submit a change of address form for your mail
  - Use “phishing” or fake emails to get you to provide personal information
  - Steal personnel records from their employers
WHAT CAN YOU DO?

• DETER
  • Deter identity thieves by safeguarding your information

• DETECT
  • Detect suspicious activity by routinely monitoring your financial accounts and billing statements

• DEFEND
  • Defend against identity theft as soon as you suspect a problem

DETER

• DETER identity thieves by safeguarding your information.
  • Shred financial documents before discarding them
  • Protect your Social Security number
  • Don’t give out personal information unless you’re sure who you’re dealing with
  • Don’t use obvious passwords
  • Keep your information secure
DETECT

- DETECT suspicious activity by routinely monitoring your financial accounts and billing statements.
- Be alert
  - Mail or bills that don’t arrive
  - Denials of credit for no reason
- Inspect your credit report
  - Law entitles you to one free report a year from each nationwide credit reporting agencies if you ask for it
  - Online: www.AnnualCreditReport.com;
  - By phone: 1-877-322-8228; or by mail
- Inspect your financial statements
  - Look for charges you didn’t make

DEFEND

- DEFEND against identity theft as soon as you suspect a problem.
- Place a “Fraud Alert” on your credit reports by calling any one of the three nationwide credit reporting companies:
  - Equifax: 1-800-525-6285
  - Experian: 1-888-397-3742
  - TransUnion: 1-800-680-7289
- Review reports carefully, looking for fraudulent activity
- Close accounts that have been tampered
- File a police report
- Contact the Federal Trade Commission
• Protect your personal information: It’s valuable
• Know who you’re dealing with
• Use all of these and update automatically
  • anti-virus software [Free from BU]
  • anti-spyware software
  • Firewall
• Set up your OS and browser securely, update automatically
• Choose strong passwords (tip!) and protect them
• Back up important files
• Learn who to contact if you have a problem

• Don’t use native password saving solutions
  • IE, Firefox, Chrome, VPN = bad
• Don’t trust unknown USB drives
• Don’t visit unknown web sites
• Remember to lock your computer every time you step away from it
  • Win + L
  • Ctrl+Alt+Del then Enter
• Think about encrypting sensitive information
MICROSOFT OFFICE SECURITY

• Sensitive information attached to documents
  • Comments, revision marks from tracked changes, versions, and ink annotations
  • Document properties and personal information
  • Headers, footers, and watermarks
  • Hidden text
  • Hidden rows, columns, and worksheets
  • Invisible content

MS OFFICE ENCRYPTION AND PROTECTION

• Encrypting a document: “password to open”

• File-sharing password: “password to modify”
  • NOT Encryption, just controls permission to change