Purdue University proudly presents

October Cybersecurity Awareness Month

Preview of October Events

- Buckle Up! Laptop Security: Scott Ksander, chief information security officer and executive director of networks and security at Purdue will share his enlightening thoughts on mobile security
- October 15th - PDA’s: “Pretty Darn Accessible” without security. Doug Couch and Nathan Heck, Security Analysts will present how to safeguard your data and privacy
More Preview of Events!

- **October 22**nd - Phones and Tech Toys: Who can hear me now? A Verizon representative and Aaron Jarvis, Purdue Network Engineer, will present how to protect your portable devices while living outside the cave.
- **October 31**st - McAfee Senior Vice Pres. of Worldwide Enterprise Business will speak and help judge the traditional Halloween Security Costume Contest

[Image of costumes with the words SecurePurdue]

[Image of a group of people in costumes]
SecurePurdue

Update

Scott L. Ksander
Executive Director, IT Networks & Security, ITaP
ksander@purdue.edu
October Cybersecurity Awareness Month

Stages of Security

- Blissfully Ignorant (20%)
- Awareness (30%)
- Corrective Action (40%)
- Operational Excellence (10%)

The Cost of Security

- Blissfully ignorant (<3% of IT budget)
- Awareness (4-6%)
- Corrective Action (7-8%)
- Operational Excellence (3-4%)

Real progress on IT security will, over time, REDUCE IT security spending requirements!
Launched 10/26/2005

2,325,525 hits to date

Redesign launched 4/3/2006
  • Hit rate since redesign – 3,800/day
  • #1 item of interest – downloads at 12%
  • #2 item of interest – news at 6%

SecurePurdue concept and web site being copied by other Big Ten institutions
SecurePurdue News

FROM the CISO
By Scott Konsard
Executive Director
IT Networks & Security
Identity theft and scams that attempt to steal your personal information have been common themes for this newsletter in the last year. Identity information continues to be a valuable commodity; however, there is some hope that the situation is improving. A recent study sponsored by a major bank and a major credit card company has released information for 2007 related to financial losses stemming from identity theft. Losses attributed to identity theft dropped 11% in 2007 to $46.3 billion. Although it is difficult to fathom losses of that magnitude, this is an improvement from the

In this issue
CISO message . . . . . . 1
Cookies . . . . . . . . . . . 2
IAMO News . . . . . . . . . . 3
Cybersecurity Events . . . . . 3
STEAM-CRT News . . . . 3
Spam, Phishing, Malware
Laden E-mails . . . . . 4
IT Outage . . . . . . . . . . . 4
Security Resources . . . . 4

Successes

- Purdue operational security recognized as experts in their field
  - EDUCAUSE
  - National media
  - National security conferences
  - Indiana Bar Association
  - U.S. Court of Appeals for the 7th Circuit
Purdue Security Officers

- Policy work
- Technical community concerned with security
- SO model being copied by other Big Ten institutions
- Policies being used as templates for other institutions

Training Opportunities

- 3 major training sessions
  - Security Essentials
  - VISTA
  - Security Web Applications
  - Attended by 155 IT staff from both WL and Regional campuses
  - $2145/person training facilitated locally for $500/person
- CISSP training (12 sessions) to provide certification option for IT staff. (materials have actually been purchased by Ivy Tech for use in their curriculum)
- Third Annual October Security Awareness Month program presented national and campus experts
**Applied Technology**

- Incident Response
  - Policy established
  - Operations capability in ITaP and a campus-wide security team (STEAM) established
  - Tools developed and deployed

---

**Applied Technology**

- Anti-virus/Anti-spyware
  - McAfee product available for campus systems and home use
  - Centralized management (ePO) continues to grow
Enhanced “border patrol”
  • Centrally coordinated firewall support
  • Intrusion detection/prevention on-line
    ➢ Over 1.5M alerts have been triggered since 7/1/2007
    ➢ 42.5% of events are attempts to gain admin access
    ➢ 13.3% were SSH account brute force attempts
    ➢ 77% of events are aimed at web applications
    ➢ Over 19,000 connections were blocked from phishing IPs associated with various “Purdue IT Team” emails
  • Completed third-party, external “Penetration Test” and incorporated lessons learned and recommendations into SecurePurdue plans

Risk Assessment
  • Risk Assessment and Security Review consulting work continues in high demand
  • Vulnerability Scanning Cluster (VSC) available for self-assessment scanning
  • AppScan tool available for web penetration testing as part of the assessments/security review process
Identity and Access Management

- Established the Authentication and Authorization policy and associated standards
- Guest account provisioning service available
- Self-service password reset application
- Increasing adoption of Career Accounts
- Deployment of “Boiler Key” for “two factor” authentication beginning next month

Good Response to Phishing

From: PURDUE WEBMAIL TEAM <support@purdue.edu>
Sent: Sat Nov 17 00:28:43 2007
Subject: Confirm Your Email Address!

Confirm Your Email Address!

Dear purdue.edu subscriber,

To complete your purdue.edu account, you must reply to this email immediately and enter your password here (*********)
Failure to do this will immediately render your email address deactivated from our database.
You can also confirm your email address by logging into your purdue.edu account at https://webmail.purdue.edu/

Thank you for using PURDUE. EDU!
THE PURDUE WEBMAIL TEAM
Community Alerted

Purdue Community warned of E-mail Scam

WEST LAFAYETTE, Ind. - The IT Networks & Security Incident Response group is warning the Purdue community about reports of a targeted e-mail scam.

The e-mail appears to come from the Purdue Webmail Team and asks users to confirm their e-mail address by responding with their password information. The e-mail also states that if the user does not respond their e-mail account will be deactivated from the database.

Real or Phishing??

From: alumnidirectory.Purdue@publishingconcepts.com
Sent: Tuesday, November 20, 2007 2:02 PM
Subject: A Nice Surprise from Purdue

Greetings from Purdue University! Because your time is valuable, we've created a personal Web site to explain what we're doing for Purdue University alumni; http://purdue.ialumni.com/PUR2520774.

Stay connected with Your Purdue network with the 2008 alumni directory. Please join us in our efforts to facilitate your connections with fellow Classmates. Visit your site as soon as you can to validate and/or update your information.

Thank you for your time,

Senior Director - Membership
Purdue Alumni Association

*** PLEASE DO NOT REPLY TO THIS EMAIL. IF YOU HAVE ANY QUESTIONS, A CONNECTIONS ASSOCIATE CAN ASSIST YOU AT THE NUMBER PROVIDED ABOVE. THANK YOU ***

Email sent on behalf of Purdue Alumni Association by PCI, 4835 LBJ #1100, Dallas, Texas 75244.
Believe that there continue to be very real threats

Awareness at all levels (faculty, staff, and students)

Meaningful, effective, and enforceable policies and procedures

Identity and Authentication as the foundation for all future identity and role based security

Effective Security Operations Center

Make security a part of every process from the beginning

A Very Active Marketplace
### Table 2. Breakdown of goods and services available for sale on underground economy servers

<table>
<thead>
<tr>
<th>Current Rank</th>
<th>Previous Rank</th>
<th>Goods and Services</th>
<th>Current Percentage</th>
<th>Previous Percentage</th>
<th>Range of Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>Bank accounts</td>
<td>22%</td>
<td>21%</td>
<td>$10-$1000</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Credit cards</td>
<td>13%</td>
<td>22%</td>
<td>$0.40-$20</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>Full identities</td>
<td>9%</td>
<td>6%</td>
<td>$1-$15</td>
</tr>
<tr>
<td>4</td>
<td>N/A</td>
<td>Online auction site accounts</td>
<td>7%</td>
<td>N/A</td>
<td>$2-$50/week—$50/week for hosting, $20 for design</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>Scams</td>
<td>7%</td>
<td>6%</td>
<td>$2-$40</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>Mailers</td>
<td>6%</td>
<td>8%</td>
<td>$1-$10</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>Email addresses</td>
<td>5%</td>
<td>6%</td>
<td>$0.83/MB—$10/MB</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>Email passwords</td>
<td>5%</td>
<td>8%</td>
<td>$4-$50</td>
</tr>
<tr>
<td>9</td>
<td>N/A</td>
<td>Drop (request or offer)</td>
<td>5%</td>
<td>N/A</td>
<td>10%-50% of total drop amount</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
<td>Proxies</td>
<td>5%</td>
<td>6%</td>
<td>$1.50-$30</td>
</tr>
</tbody>
</table>

Source: Symantec Corporation
October Cybersecurity Awareness Month

---

**Black Market Model**

- $100M market profits in 2007
- Number of markets: Increasing
  - Market liquidity: Increasing
    - Number of records traded is soaring
    - Number of criminals participating is soaring
  - Price of identity: Decreasing
    - 2002: $150
    - 2007: $14 (10X DECREASE)
  - Quality of goods: Increasing
    - Identities rated by credit limit
    - Fully qualified with SSN, DOB, passwords, and “COB” (Change of Billing) guaranteed
Buckle Up!
Laptop Security

Scott L. Ksander
Executive Director, IT Networks & Security, ITaP
ksander@purdue.edu
Lost Laptops

- 53% of mobile professionals carry confidential company information on the laptop and, of those, 65% don’t take steps to protect the data
- Lost or stolen laptops are the most frequent cause of a data breach, accounting for 49% of data breaches in 2007
- 20% of customers terminate the relationship after a data breach

Lost Laptops

- 12,255 lost laptops per week at US airports
- 97% are NEVER recovered
- Some common destinations
  - LAX – 1,200/week
  - SFO – 350/week
  - ORD – 825/week
  - DCA – 450/week
  - IND – 30/week
Lost Laptops

- Security Checkpoints – 40%
- Departure gate – 23%
- Restroom – 9%
- Food Service – 7%
- Club or Lounge – 6%
- Transportation system – 6%

Rules of the Road

- Never leave your laptop unattended
- Never check your laptop in your luggage
- Record identifying information and mark your equipment
- Consider “phone home” protection software
- Downplay your laptop
Not The Best Choice …

To paraphrase James Carville,

*It’s the data, stupid!!*
It’s The Data ...

- Know where the data lives
- If you must carry sensitive or restricted information, encrypt it
- Better yet, carry the data as securely as possible
  - Securely access the data from secure storage
  - Use encrypted USB devices

ENCRIPTION!!

- Simple methods are effective
  - PKZIP
  - TrueCrypt
  - IronKey
When Travelling By Air

- If there is a sudden diversion in front of you, a laptop thief is probably behind you
- Look out for 2 person scams
- Don’t check laptops as luggage
- Don’t put laptops in the overhead bins
- Laptops in seatback pocket are prohibited
- Keep the case by your feet and in sight

When Travelling By Car

- Never leave your laptop in a rental car
- Never leave your laptop visible in your own car
When Staying in a Hotel

- Lock the laptop with a cable or in a safe when you are not in your room
- Treat it as you would a book of signed checks
- Take it with you whenever possible

When At A Conference

- Laptop thieves target business conferences and conventions because they know you will feel comfortable around your peers
- Never leave your equipment in an unlocked or unmonitored room
Controlled Access

- Disable IR ports
- Disable Bluetooth
- Disable 802.11 a/b/g/n

Don’t make access easy

- Disable Auto-Logon
- Disable Guest Account
- Keep administrative password for very special circumstances
- Use OS-based access controls
- Enable OS-based firewall with most restrictive settings
Wandering Eyes

- Shoulder surfing
- Screen guards

A Layered Approach

- Understand the risks
- Be proactive
- Install anti-virus and anti-spyware
- Backup data so you can determine what is missing
- Assume your laptop will be lost or stolen and create a contingency plan
Road Warrior Wi-Fi

- Turn off adapter when not in use
- Verify SSID for service provider
- Verify firewall enabled on wi-fi
- Disable file and printer sharing
- Keep system, application, and drivers up to date
- Use VPN technology

Make Security a Habit

- Connect Securely
- Tunnel Safely
- Surf Encrypted
- Password Strongly
- Speak Nothing, Trust No One