Exceptional service in the national interest

SAND2013-3062C

Cyber Security

Protecting PII & PHI

By Nick Peterson and Dominic Salas

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Presentation Goals

- Importance of protecting sensitive data
- Threats that put your data at risk
- Improving your understanding of Computer Security
- Provide useful information you can use to protect data

Overview of PHI & PII

- What is PHI?
  - Personal Health Information
  - Health information and individually identifiable health information (MR#, Device identifiers and serial numbers, etc.)
- What is PII?
  - Personally Identifiable Information
  - Any information that can be used to identify an individual (SSN, DOB, Passport #, etc.)
- How are they related?

Why is PHI a target?

- Identity Theft
- Insurance Fraud (Medicaid, Medicare, etc.)
- Expose a patient's illness
- 932,544 records compromised in 2012
  - 321,426 in 2013 (privacyrights.org)
- Black Market Value
  - A medical record sells for $50
  - Just $1 for Social Security Number (SSN)

Threats

- Unauthorized physical access
- Social Engineering
- Phishing
- Viruses/Malware
- Web Attacks
- Mobile Security

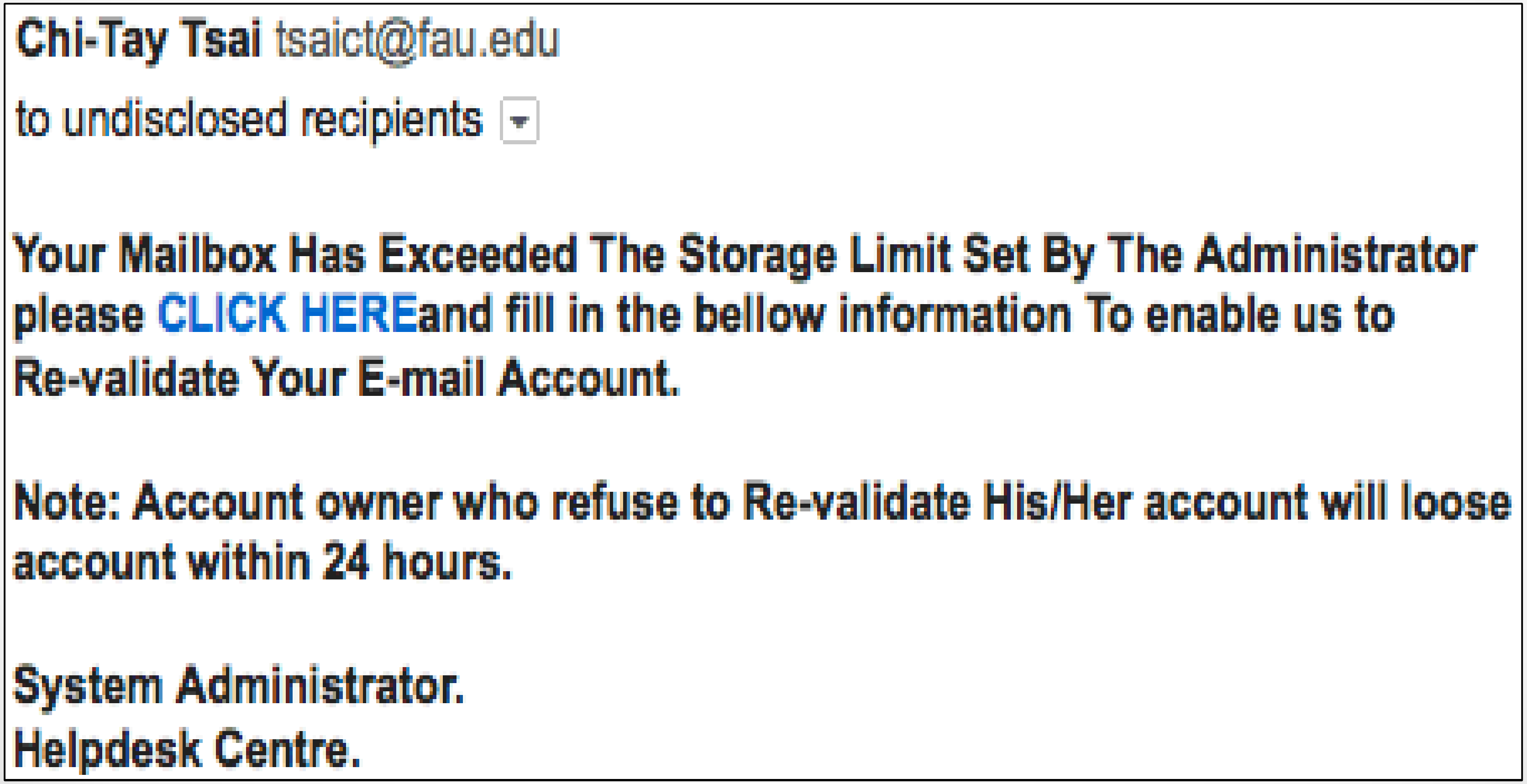
Unauthorized Physical Access

- All bets are off if physical access is gained
- How does it happen?
  - Unlocking computer without a password
  - Recording keyboard input
  - Cracking password
  - Accessing unencrypted data
- What damage can be done?
  - Loss of PII / PHI
  - Identity theft
  - Blackmail
  - Change information
  - Availability

Social Engineering

- Manipulating people into performing actions or divulging confidential information (CON ARTIST)
- High profile example
  - England case involving Kate, Royal Family, nurse, PHI

Suspicious Email?



Chi-Tay Tsai tsaict@fau.edu

to undisclosed recipients ▾

Your Mailbox Has Exceeded The Storage Limit Set By The Administrator please CLICK HEREand fill in the bellow information To enable us to Re-validate Your E-mail Account.

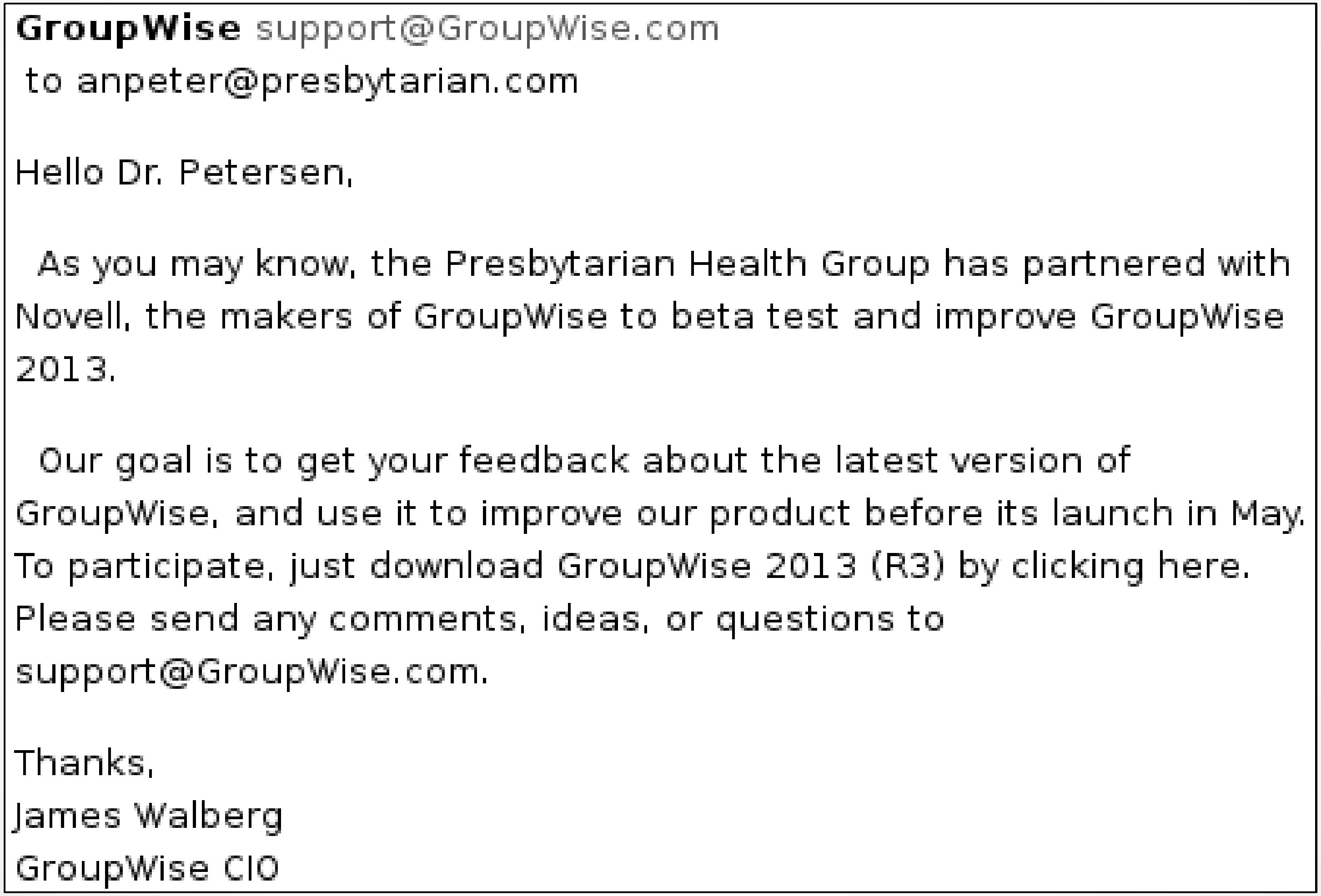
Note: Account owner who refuse to Re-validate His/Her account will loose account within 24 hours.

System Administrator.
Helpdesk Centre.

Phishing

- Emails sent by an attacker posing as a trustworthy entity to steal your personal information
- Indicators of a phish
  - Grammar
  - Spelling
  - Capitalization
  - Unknown sender
  - Lack of personalization
  - Threatening language
  - Undisclosed Recipients

Advanced Phish?



GroupWise support@GroupWise.com
to anpeter@presbytarian.com

Hello Dr. Petersen,

As you may know, the Presbytarian Health Group has partnered with Novell, the makers of GroupWise to beta test and improve GroupWise 2013.

Our goal is to get your feedback about the latest version of GroupWise, and use it to improve our product before its launch in May. To participate, just download GroupWise 2013 (R3) by clicking here. Please send any comments, ideas, or questions to support@GroupWise.com.

Thanks,
James Walberg
GroupWise CIO

Spear-Phishing

- Phishing targeted at an individual or small group. Uses specific information relevant to only the target.
- Indicators of a Spear-Phish
  - Unexpected correspondence
  - Position of authority
  - Appears to be from known sender
  - Personalized
  - Relevant to existing work/projects
  - Out of character

Virus/Malware

- Malicious software
  - Steal username/password
  - Steal PHI/PII
  - Steal financial information
  - Destructive/Disruptive
  - Ransomware/Scareware

How do you get infected?

- Unpatched software
- Running unknown software
  - Email attachments
- Sharing thumb drives
- Browsing the internet
  - Compromised trusted websites

Mitigations

- Patching
- Separation of tasks
- Safe Browsing Techniques
- Protective Software
- Encryption
- Passwords

Patching…

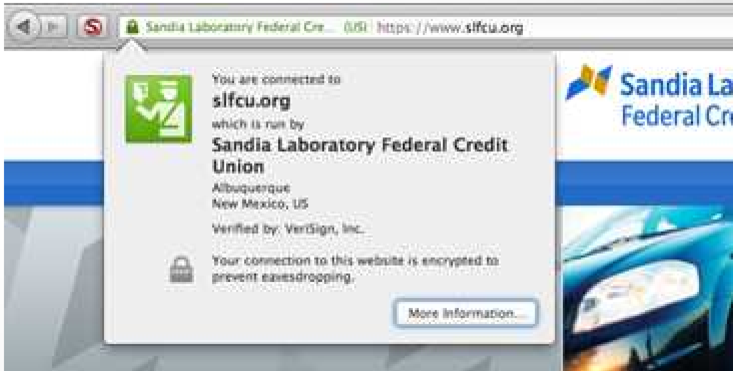
- Keeping your computer up to date
  - Time critical
- Helpful Software
  - Turn on automatic system updates
  - Secunia PSI / Avast Free
    - 3rd party update notifications
    - Automatic Updates

Separation of tasks

- Keep risky activities away from your sensitive data
- Use one computer for
  - Financial information
  - PII/PHI
- Use another for
  - Kids
  - Recreational browsing
  - Gaming
  - Suspicious programs
  - Email

Safe Browsing

- Alternate web browser
    - Chrome or FireFox
- Login page uses encryption
    - https:// in address
- Don’t install software you didn’t seek out



You are connected to
slfcu.org
which is run by
Sandia Laboratory Federal Credit Union
Albuquerque
New Mexico, US

Verified by: VeriSign, Inc.

Your connection to this website is encrypted to prevent eavesdropping.

Anti-Virus

- Useful, but not bulletproof
  - More exploits being discovered
  - Anti-virus takes time to catch up
  - Effective against older viruses
- Offers additional protections
  - Anti-phishing
  - Auto-patching
  - Website Reputation
- Free Versions
  - Microsoft Security Essentials
  - Free AVG
  - Avast!

Encryption

- Encryption at rest
  - o BitLocker (windows)
  - o FileVault (mac)
  - o Office 2010 & above
    - FIPs 140 Compliant (federal standard)
- Encryption in transit
  - o Secure webpage (https://)
  - o Office 2010 & above

Passwords

- Password Strength
  - Machine generated (GRC.com)
- Password Reuse
- Password Vaults
  - LastPass
- PassPhrases
  - I.e. Squirrels paint lackadaisically during summer
- Periodically changing passwords
- Password recovery questions

Questions?

Misc. Protections

- Microsoft EMET (free)
  - Defeats modern attacks
- Microsoft Steady State
  - Prevents modification across reboots

Mobile Devices (Bonus Material)

- Avast Application for Android
- New Nexus 4 allows for full disk encryption
- Password protecting phone
  - Password protect SIM
  - Lock screen
- Remote wipe

Tools Covered

What to do	Tool to help	What the tool does
Keep software updated	Secunia	Automatically updates your software (Free)
Don't re-use passwords	LastPass	Stores usernames & passwords so you don't have to (Free)
Only install trusted apps	Avast Mobile (Android)	Warns you before installing malicious apps that may steal your data. (Free)
Use anti-virus	Avast	Detects known viruses helping to protect your computer from infection. (Free)
Encrypt entire hard drive	Microsoft BitLocker (Win) Apple FileVault (Mac)	Makes computer useless to thieves, protecting PII. (Free)
Make sure website uses encryption (https://)	HTTPS Everywhere	Enforces Encryption on sites that support it. (Free)
Enable remote wipe on your mobile devices	MobileMe (iPhone) Avast Mobile (Android)	Allows you to erase or find your phone / tablet if lost (Free)