

Fermilab Computer Security Awareness Day

# **BASIC COMPUTER SECURITY**

# Why Computer Security

- ◎ The Internet is a dangerous place
  - We are constantly being scanned for weak or vulnerable systems; new unpatched systems will be exploited within minutes.
  - Becoming more frequent are phishing attacks on users.
- ◎ Fermilab is an attractive target
  - High network bandwidth is useful for attackers who take over lab computers
  - Publicity value of compromising a .gov site
  - Attackers may not realize we have no information useful to them

# Why Computer Security

- ⦿ Security depends on everyone, from management, to system administrators to users.
  - As mentioned, phishing attacks are more prevalent
  - Three DOE labs taken offline earlier this year due to phishing attacks
  - A chain is only as strong as its weakest link
- ⦿ Integrated Security Management
  - Part and parcel of everything you do with computers (analogy with ES&H)

# Email: Spam

- ◎ Everyone gets spam all the time
- ◎ In 2007, it was estimated that 85% of incoming email was “abusive email”
- ◎ A 2010 survey of US and European email users showed that 46% of recipients opened spam messages and 11% clicked on a link

# Top five spam subject lines

- ⦿ Bogus online orders (“Order N21560”).
- ⦿ Fake fines (“FW: Re: UNIFORM TRAFFIC TICKET (ID: 239127922)”)
- ⦿ Package delivery lies (“USPS Invoice copy ID46298”)
- ⦿ Tests for working addresses (often are blank emails)
- ⦿ Payment and tax cons (“FRAUD ALERT for ACH”)

# Email: Phishing

- ⦿ Goes hand-in-hand with spam
- ⦿ Let's take a look at an example email

Date: Sun, 06 Nov 2011 01:50:15 -0500  
From: IT Service Desk <tech.team@tech-center.com>  
Reply-to: itservicecenter@tech-center.com  
To: undisclosed-recipients: ;  
Subject: Scheduled Maintenance & Upgrade

IT Service Desk

Attn account User,

Scheduled Maintenance & Upgrade

Your account is in the process of being upgraded to a new set of Windows-based servers and an enhanced online email interface inline with internet infrastructure Maintenance. The new servers will provide better anti-spam and anti-virus functions, along with IMAP Support for mobile devices that Support IMAP to enhance your usage.

To ensure that your account is not intermittently disrupted but active during and after this upgrade, you are required to kindly confirm your account by stating the details below:

\* User name:  
\* Password:

This will prompt the upgrade of your account.

Failure to acknowledge receipt of this notification, might result to a temporal deactivation of your account from IT Service Desk database.

Your account shall remain active upon your confirmation of your login details.

IT Service Desk apologize for any inconvenience caused.

IT Service Desk

Copyright 2011, All Rights Reserved.

# Email: Phishing

- ⦿ Do any red flags jump out?
- ⦿ How about sender's email address or what they are requesting?
- ⦿ Sometimes things are trickier than they seem.

**From:** Rizzo, Brian [mailto:brizzo@westfield.ma.edu]

**Sent:** Friday, November 18, 2011 11:09 AM

**Subject:** Warning! deactivation of email address

Dear User,

As part of our regular maintenance done on the exchange mail servers, Microsoft System Administration is currently working to improve on the security, functionality and performance of all our Microsoft Outlook Webmail Access Accounts as we periodically review certain Accounts which are vulnerable to Unauthorized Access or has not been used or accessed over a period of time will be deleted to conserve storage. However, your Account has been detected and queued up to be deleted from our DB. Please note that the mail in the deleted mailboxes will NOT be recoverable.

To remove this limitation and initiate your Account Update and activation process, please click [here](#) and complete the request Form.

Thank you for your co-operation  
Webmail Management Team



<https://docs.google.com/spreadsheet/viewform?formkey=dE1QdjFLamNrQ0lYdm81UWNlNGlwNFE6MQ>

# Maintenance Webmail System Administrator

WARNING! Protect your privacy. Logout when you are done and completely exit your browser.

\* Required

**User Name: \***

**Password: \***

**Confirm Password: \***

**e-Mail ( i.e info@domain.com) \***

Powered by [Google Docs](#)

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)

# Email

- ⦿ The purpose of sending spam or phishing essentially comes down to money (now or later):
  - Obtaining bank account information
  - Your machine becomes compromised and becomes a member of a botnet
  - Your email account compromised to send more spam.
- ⦿ Be careful on what you click on and what you reply to!

# Web browsing

- ① We know that clicking a link in an email can be bad – this applies to general web browsing as well.
- ① What happens if you see the following screen when browsing the web at Fermi?



Questions? Read the [FAQ](#)

## BEWARE: YOUR MACHINE MAY BE COMPROMISED WHEN VISITING THIS SITE

You are attempting to visit a web site that has been detected as possibly delivering or supporting:

- Fake Antivirus alerts
- System compromise attempts
- Exploiting vulnerabilities in web browsers
- Malicious executable downloads
- Phishing and scams
- Spyware, Malware or other potentially malicious software

If you believe you are receiving this notice in error, please speak with your manager or supervisor to have the issue escalated or open a [Helpdesk ticket](#) assigned to your supervisor with the following information:

- Your contact information
- Date and time when you received this error
- Your machine name and IP address
- The web site you were attempting to contact
- Cite reasons why denial of access to this web site interferes with your operations

If you wish to continue to the intended website, please be advised that due to reports of active exploits delivered from this site **MAY RESULT IN A COMPROMISE OF YOUR COMPUTER WHICH WILL REQUIRE A RE-INSTALL OF YOUR OPERATING SYSTEM AND APPLICATIONS.**

If you accept this risk and wish to continue to the intended web site, please acknowledge this warning by clicking [Accept](#) or press your browser's BACK button to exit.

**Please note that this action will be logged.**

# Incidental Computer Usage

- ⦿ Fermilab permits some non business use of lab computers
- ⦿ Guidelines are at <http://security.fnal.gov/ProperUse.htm>
- ⦿ This is pretty much common sense

# Social Engineering

- ⦿ Not every method to give up electronic data is electronic.
- ⦿ Phone calls
- ⦿ In person
  - Or physical media

# Passwords

- ⦿ Always choose a complex password
  - The lab has a password policy that's enforced, so it's difficult to choose a weak Fermi password.
- ⦿ Differentiate your passwords
- ⦿ Change them periodically (yes, even passwords to personal accounts).

# The top 25 worst passwords revealed (Nov 2011)

- |                     |                     |
|---------------------|---------------------|
| 1. <u>password</u>  | 14. <u>master</u>   |
| 2. 123456           | 15. <u>sunshine</u> |
| 3. 12345678         | 16. <u>ashley</u>   |
| 4. <u>qwerty</u>    | 17. <u>bailey</u>   |
| 5. <u>abc123</u>    | 18. <u>passwOrd</u> |
| 6. <u>monkey</u>    | 19. <u>shadow</u>   |
| 7. 1234567          | 20. 123123          |
| 8. <u>letmein</u>   | 21. 654321          |
| 9. <u>trustno1</u>  | 22. <u>superman</u> |
| 10. <u>dragon</u>   | 23. <u>qazwsx</u>   |
| 11. <u>baseball</u> | 24. <u>michael</u>  |
| 12. 111111          | 25. <u>football</u> |
| 13. <u>iloveyou</u> |                     |

# Fermilab and Central Authentication

- ⦿ All use of lab computing services requires central authentication
- ⦿ Avoid disclosure of passwords on the network
- ⦿ No network services (logon or read/write ftp) visible on the general internet can be offered without requiring strongest authentication, currently Kerberos (unless a formal exemption is applied for and granted)
- ⦿ Kerberos provides a single sign in, minimizing use of multiple passwords for different systems
- ⦿ Lab systems are constantly scanned for violations of this policy

# What happens if you notice a Computer Security incident?

- ◎ Mandatory incident reporting;
  - Report all suspicious activity:
    - *If urgent* to the Service Desk, x2345, 24x7;
    - *Or* to system manager (if immediately available);
    - Non-urgent to [computer\\_security@fnal.gov](mailto:computer_security@fnal.gov);
  - Incidents investigated by Fermi Computer Incident Response Team (FCIRT);
  - *Not* to be discussed!

# FCIRT (Fermi Computer Security Incident Response Team)

- ⦿ Security experts drawn from throughout the lab
- ⦿ Investigate (“triage”) initial reports;
- ⦿ Coordinate investigation overall;
- ⦿ Work with local system managers;
- ⦿ Call in technical experts;
- ⦿ May take control of affected systems - for an undetermined amount of time;
- ⦿ Maintain confidentiality;

# Integrated Security Management

- ⦿ Computer Security is not an add-on or something external, it is part and parcel of everything you do with computers (analogy with ES&H)
- ⦿ Not “one-size-fits-all” but appropriate for the needs and vulnerabilities of each system
- ⦿ In most cases, it is simply common sense + a little information and care
- ⦿ Each Division/Section or large experiment has a GCSC (General Computer Security Coordinator) who acts as liaison with the Computer Security Team in disseminating information and dealing with incidents; see <http://security.fnal.gov/> for an up to date list

# Perimeter Controls

- ⦿ Certain protocols are blocked at the site border (email to anything other than lab mail servers; web to any but registered web servers; other frequently exploited services)
- ⦿ Temporary (automatic) blocks are imposed on incoming or outgoing traffic that appears similar to hacking activity; these blocks are released when the activity ceases (things like MySpace and Skype will trigger autoblocker unless properly configured)

# Patching and Configuration Management

- ⦿ Baseline configurations exist for each major operating system (Windows, Linux, MAC)
- ⦿ All systems must meet the baseline requirements and be regularly patched (in particular running an up-to-date supported version of the operating system) UNLESS:
  - A documented case is made as to why the older OS version cannot be upgraded
  - Documentation exists to demonstrate that the system is patched and managed as securely as baseline systems
  - All non essential services (such as web servers) are turned off
- ⦿ All systems with Windows file systems must run anti virus
- ⦿ Your system administrator should take care of this for your desktop

# Critical Vulnerabilities and Vulnerability Scanning

- ⦿ Certain security vulnerabilities are declared critical when they are (or are about to) being actively exploited and represent a clear and present danger
- ⦿ Upon notification of a critical vulnerability, systems must be patched by a given date or they will be blocked from network access
- ⦿ This network block remains until remediation of the vulnerability is reported to the TISSUE security issue tracking system (as are blocks imposed for other security policy violations)

# Prohibited Activities

- ◎ “Blatant disregard” of computer security;
  - First time perhaps only warning, repeat offense disciplinary action;
- ◎ Unauthorized or malicious actions;
  - Damage of data, unauthorized use of accounts, denial of service, etc., are forbidden;
- ◎ Unethical behavior;
  - Same standards as for non-computer activities;
- ◎ Restricted central services;
  - May only be provided by approved service owners;
- ◎ Security & cracker tools;
  - Possession (& use) must be authorized;
- ◎ See <http://security.fnal.gov/policies/cpolicy.html>

# Activities to Avoid

- ⊙ Large grey area, but certain activities are “over the line”;
  - Illegal;
  - Prohibited by Lab or DOE policy;
  - Embarrassment to the Laboratory;
  - Interfere w/ performance of job;
  - Consume excessive resources;
- ⊙ Example: P2P (peer to peer) software like Skype and BitTorrent: not explicitly forbidden but very easy to misuse!

# Questions?

- ◎ [nightwatch@fnal.gov](mailto:nightwatch@fnal.gov) for questions about security policy
- ◎ [Computer\\_security@fnal.gov](mailto:Computer_security@fnal.gov) for reporting security incident
- ◎ <http://security.fnal.gov/>