Information Security Training for XSEDE Researchers
Developed by XSEDE Security Operations
James A. Marsteller, PSC

XSEDE
Extreme Science and Engineering Discovery Environment

September 6, 2017
Training Overview

- Security Awareness
- You Are The Target
- Social Engineering
- Email and Instant Messaging
- Using Your Browser Safely
- Passwords

- Encryption/Data Protection
- Mobile Devices
- Protect Your Computer
- Wi-Fi Security
- Reporting a Security Incident
Security Awareness

• Nothing is ever *truly secure*

• Your environment is constantly changing. You must prepare - recognize - respond

• Security is an **on-going process** that is reviewed and adjusted based on the changing variables.
Common Misconceptions

• “Security is a Technical Problem that is hard to understand”
• “Security should be left to specialists in Information Technology”

Reality: Security Is Everyone’s Responsibility
Why you should care?
Because you are the target...

Attackers want:

• Your personal information
• Your network connection
• Your computer/resource
Why Your Help Is Needed

Source of Security Events

- XSEDE Researcher/User
- Other
Infected computers and security breaches can lead to:

- **Poor Performance**: A computer using some of its resources to run malware means less resources for you to use.
- **Identity Theft**: Stealing your personal information to commit fraud or theft.
- **Questionable research data**: Stolen, destroyed or modified data. How can you tell that “0” should be a “1”?
- **Public Image/Reputation**: Impact personal or organizational reputation, could affect future funding opportunities.
- **Liability**
- **Breach of contractual agreements** (non-disclosure agreements)
Your Role In Security

• You are the last line of defense!
• The majority of security events can be traced back to improper credential management and/or compromised user desktops/laptops.
• Equip yourself with the knowledge of your local security guidelines, policies, and procedures as well as XSEDE Policies
• Know who to call locally for security assistance
Social Engineering

Is the art of manipulating people into performing actions or divulging confidential information.

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.

Examples:

- Phishing activities
- Phone calls from the “Microsoft Security Team”
Social Engineering

**Phishing** attacks use e-mail, instant messages or malicious websites to solicit personal information by posing as a trustworthy organization

- Impersonation of trusted contacts
- Epidemics and health scares (e.g., H1N1)
- Economic concerns (e.g., IRS refund scams, Stimulus $$ )
- Major political elections
Social Engineering - Understand How They Manipulate You:

**Fear** – ‘you’ll loose your e-mail service’, ‘past due invoice’, must open an attachment

**Exclusivity** – Invite to a new on-line service

**Guilt** – Sick child (make a wish), war victims needing help

**Greed** – IRS refund, won lottery/contest, Mysterious Benefactor

**Ego Satisfaction** – ‘Who’s Who Registry Confirmation’, conference invitation
Email and Instant Messaging

• Don't open attachments that you weren’t expecting to receive and make sure to scan attachments with antivirus software.

• Trust your instincts! If an e-mail or attachment seems suspicious, don't open it. Forward to security staff.

• Contact organizations by phone to verify if action is needed: banks, credit card companies, PayPal, etc.
Email and Instant Messaging

• Don't send sensitive information via email!

For example, never send:

– **Account names & passwords**
– Credit card numbers
– Social Security, personal information
  (birthdate, mother’s maiden name, etc.)

Think of email as a postcard written in pencil. It can be read by 3\textsuperscript{rd} parties and possibly altered.
Email and Instant Messaging

Don't click links within emails without checking for masquerading.

Most email clients will show link information by placing the cursor over the link/URL in the email.
Using Your Browser Safely

• Be very careful of anything you download to your computer and make sure to scan the software before you open or install.
• Apply updates and avoid untrusted plug-ins
• Disable Flash in your browser or use “Click to flash” to prevent automatic running of flash files on websites.
Using Your Browser Safely

- Use Secure HTTP (HTTPS) when entering sensitive information on websites
Using Your Browser Safely

Heed warning of malicious websites
Passwords

• Easy for you to remember but difficult for others to guess
• Don’t share your password with others
• Use different passwords for each account
• Avoid security question answers that can be easily answered by searching social networks. “Where did you first work?” Checking for a LinkedIn profile may reveal this answer.
Selecting Strong Passwords

- Use at least 8 characters long and include non-alphabetical characters like numbers and symbols (!@$)

- Using passphrases can help remember complex passwords. Use the first letter in a phrase: **Mswbof7702** = “My son was born on Friday July 7th 2002”

- Use multifactor Authentication where possible
Password Management Tools

- Consider using software to securely manage passwords on your desktop/mobile device.
Some suggestions:

KeePass
Free (Open Source)
http://keepass.info

Password Vault
http://www.lavasoftware.com/passwordvault.html

1Password
https://agilebits.com/onepassword
<table>
<thead>
<tr>
<th>Password</th>
<th>Password</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>123456</td>
<td>987654321</td>
<td>555555</td>
</tr>
<tr>
<td>123456789</td>
<td>qwertyuiop</td>
<td>3rjs1la7qe</td>
</tr>
<tr>
<td>qwerty</td>
<td>mynoob</td>
<td>google</td>
</tr>
<tr>
<td>12345678</td>
<td>123321</td>
<td>1q2w3e4r5t</td>
</tr>
<tr>
<td>111111</td>
<td>666666</td>
<td>123qwe</td>
</tr>
<tr>
<td>1234567890</td>
<td>18atcskd2w</td>
<td>zxcvbnm</td>
</tr>
<tr>
<td>1234567</td>
<td>77777777</td>
<td>1q2w3e</td>
</tr>
<tr>
<td>password</td>
<td>1q2w3e4r</td>
<td></td>
</tr>
<tr>
<td>123123</td>
<td>654321</td>
<td></td>
</tr>
</tbody>
</table>

Source: https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/
Only Use Your XSEDE Account on XSEDE Resources

• Make sure Domain is “XSEDE.ORG” in URL field of your browser (e.g. Good: http://portal.xsede.org”)

• XSEDE will NEVER ask you for your password.
Using Two Factor Authentication with DUO

• **Choose to protect** SSH login attempts to your accounts at certain XSEDE Service Providers that have implemented XSEDE Two Factor Authentication (XSEDE TFA) XSEDE portal account username/password as the primary authentication factor + Duo Security Authentication as the secondary authentication factor.

• Currently, SSH access for the following XSEDE systems can be protected in this fashion.
  – XSEDE SSO (Single SignOn) Hub at login.xsede.org
  – NICS Darter SP – duo.darter.nics.xsede.org
  – PSC Bridges – bridges.psc.xsede.edu

• To enroll in DUO look for the DUO logo shown below in your XSEDE User Profile page

• For more detailed information about DUO visit the DUO user guide.
  https://guide.duo.com
Using Two Factor Authentication with DUO
Why Encrypt Data?

• Legal, financial, and public reputation liabilities
• Overseas travel
• Travel back into the United States
  – “Federal agents may take a traveler's laptop computer or other electronic device to an off-site location for an unspecified period of time without any suspicion of wrongdoing, as part of border search policies”
    (http://www.washingtonpost.com/wp-dyn/content/article/2008/08/01/AR2008080103030.html)

• Personal privacy
  – Photos, family documents, etc.
What data needs to be encrypted?

- Social security, driver’s license, and credit card numbers
- Grades/G.P.A information
- Salary information
- Staff performance reviews
- Personally identifiable information about human research subjects
- Health or medical record information
What data needs to be encrypted? (cont.)

- Information protected under Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA) protected information
- Information obtained from a third-party under a written obligation of non-disclosure or confidentiality
- Other non-public personally identifiable information (W-2 info., home phone, DoB)
XSEDE Acceptable Use Policy (AUP)

When XSEDE approves your request for resources, you must digitally sign the XSEDE Acceptable Use Policy the first time you log into the XSEDE User Portal at the beginning of each allocation. You must do this within 30 days of the approval of your allocation, or your account will be deactivated.

Your on-line acceptance is your acknowledgment that you have read and understand your responsibilities as a user

AUP Policy - https://www.xsede.org/usage-policies
XSEDE User’s Responsibility for Data

“It is your responsibility to be aware of the laws and policies that are associated with the data you are managing and to verify that the XSEDE RP site used can provide the appropriate level of protection.” – XSEDE User Responsibility Agreement

XSEDE does not provide security or protection for HIPPA, FERPA, GLBA, Classified or Export Controlled data
XSEDE User’s Responsibility

“You will not use XSEDE-allocated resources for financial gain or any unlawful purpose, nor attempt to breach or circumvent any XSEDE administrative or security controls.”
Principal Investigator (PI) Responsibilities

• You are responsible for your allocation usage
• Verify and Vet requests and identities for new users
• PI's will also ensure that users follow the XSEDE AUP
• Maintain accurate collaborator information on your allocation
  – Remove users when collaboration ends
  – Do not share access (do not reuse XSEDE credentials, for example Teaching Assistants).
• Report any usage inconstancies
How do I encrypt data?

- Some Operating Systems support data encryption (MacOS ‘Filevault’, Windows ‘Bitlocker’)
- Commercial offerings available
Securing Mobile Devices

- Password protect your phone/tablet
- Use autowipe after numerous failed attempts
- Use Encryption if possible
- Use “find my phone” software & remote wipe
- Only add Apps from trusted sources
- Disable Bluetooth if not needed
- Avoid using untrusted power sources (power port also used for data communications and transfers). Use USB sync blocker.
Protecting Your Computer Checklist:

- Seek support from your local system administrators
- Be cautious with USB sticks, other foreign hardware
- Create a separate non-admin account for your daily usage. Only use the admin account when needed.
- Make an informed and rational decision prior to installing or downloading software on your computer – if unsure ask security staff
- Disable file sharing
Protecting Your Computer Checklist:

- Enable your Firewall and seek advice of security staff when modifying firewall policy
- Patch and update your operating system (including non-OS software – Adobe Flash/Reader, Java, Browsers)
- Install and update your anti-virus and anti-malware with the latest security definitions
- Enable a password protected screen saver to prevent unauthorized use
Wi-Fi Security

• Assume public wi-fi networks are NOT SECURE
• Use a VPN supplied by your organization if possible
• Turn Off any sharing (file, photo, iTunes, p2p)
• Use HTTPS for surfing and SSL for email/other tasks
• Make sure your firewall is operating
Social Networking

- Assume everything you post is public and cannot be erased
- Avoid posting when you'll be away from home
- Be aware of scams
- Can be used for finding answers to security questions (FB, LinkedIn)
- Installing FB apps can share all of your FB data with the developer, same for your friends
Detecting a compromise

A computer experiencing unexpected and unexplainable:

- Unusual Disk activity
- Performance degradation
- Repeated login failure or connections to unfamiliar services
- Third party complaint of a suspicious activity
- If your computer/laptop/mobile device is stolen
Reporting a Security Incident

If you believe your XSEDE account (or computer you use) may have been compromised:

1. STOP!

2. Contact local Security Staff and/or systems administrator

3. Notify the XSEDE Helpdesk 1-866-907-2383 or ‘help@xsede.org’

Make sure to report stolen computers!
Key Take-a-ways

- YOU play a significant role in security
- Choose strong passwords and don’t share them between accounts or with others
- Utilize your local security team for advice and guidance
- Keep your computer properly patched and protected (anti-virus, Firewall enabled, etc.)
- Report any security concerns to XSEDE staff ASAP
More Information....

• Email: security-lead@xsede.org

• XSEDE Security homepage
  https://www.xsede.org/security

• Online security tutorial via CI Tutor
Our reach will forever exceed our grasp, but, in stretching our horizon, we forever improve our world.

XSEDE
Extreme Science and Engineering Discovery Environment