

1) Send an email to an OTT Director or Branch Chief, requesting approval for VPN access. Once approval is received via email, forward to Sharon Fields or NED requester for processing. The NED requester will work with AO to obtain approval.

2) Complete online course on the following screens below.

click here <http://irtsectraining.nih.gov/>

The screenshot shows the NIH Information Security and Privacy Awareness Training login site. The header includes the NIH logo and the title "NIH INFORMATION SECURITY AND PRIVACY AWARENESS TRAINING". Below the header is a "NIH LOGIN SITE" section. On the left, there is a "Login for NIH:" section with a list of user types: Employees, Contractors, Fellows, NIH Guests or Tenants, Special Volunteers, and New staff coming to NIH. Below this list is the text "Who use NIH Information Systems." In the center, there is a "NIH ID Number:" section with the instruction "Your ID is the same as the 'Personal Identifier' on the back of your NIH badge." Below this instruction are two images of NIH badges. The first is a standard NIH badge, and the second is a badge with a "Personal Identifier" field highlighted in red. Below the images is a "SEARCH FOR YOUR NIH ID" section with a magnifying glass icon and a list of user types: Staff without an NIH ID badge, New staff scheduled to begin working at NIH, and Staff who forgot their NIH ID. Below the list is a "Click Here" link. At the bottom of the login site, there is a "ENTER NIH ID NUMBER:" section with three input fields containing "001", "2100", and "000". Below these fields is a red banner that says "NIH STAFF CLICK HERE TO ENTER NIH TRAINING SITE". At the bottom left, there is a "PUBLIC ACCESS TO NIH COURSES NOT FOR NIH STAFF" section with an "Enter Here" link. At the bottom right, there is a "System Requirements" link with the text "Pop-up blocker must be disabled to view System Requirements."

The screenshot shows the NIH Information Security and Privacy Awareness Training user verification screen. The header includes the NIH logo and the title "NIH INFORMATION SECURITY AND PRIVACY AWARENESS TRAINING". Below the header is a "USER VERIFICATION:" section with the question "Is this you?\*" and a table of user information. The table has three columns: Name, NIH ID #, and SAC. The first row shows "THANH NGUYEN", a redacted NIH ID #, and "HNA46". Below the table are "YES" and "NO" buttons. Below the buttons is the text "Click Yes to confirm that the user information shown is yours and continue." and "Click No to return to the login screen and re-enter your badge ID number." At the bottom, there is a note: "\*If the Name is blank: This means your Administrative Officer entered you into the NIH Enterprise Directory (NED) today. This system will update tonight and you will be able to take your training tomorrow." A red arrow points to the "YES" button.

Name	NIH ID #	SAC
THANH NGUYEN	[REDACTED]	HNA46



## WELCOME TO THE NIH INFORMATION SECURITY AND PRIVACY TRAINING COURSES

PLEASE MAKE A SELECTION:

LOG OUT

VIEW MY STUDENT RECORD

Pop-up blocker must be disabled to view

Course Title	Completed?
<b>MANDATORY COURSES FOR ALL NIH STAFF</b>	
<b>Information Security Awareness</b>	
<a href="#">Entire NIH Information Security Awareness Course:</a> Required prior to or immediately upon entry to NIH	YES
<a href="#">2012 NIH Annual Security Refresher:</a> Required annually after taking the entire course	YES
<b>Privacy Awareness</b>	
<a href="#">Entire NIH Privacy Awareness Course:</a> Required prior to or immediately upon entry to NIH	YES
<a href="#">2012 NIH Annual Privacy Refresher:</a> Required annually after taking the entire course	YES
<b>SPECIALIZED TRAINING COURSES</b>	
<b>Users Requesting Remote Access</b> (additional IC approvals apply)	
<a href="#">Securing Remote Computers</a>	YES
<a href="#">Remote Access User Certification Agreement</a>	11/03/2009
<b>Users Requesting Administrative Rights to their Computers</b> (additional IC approvals apply)	
<a href="#">FDCC Systems Administrator Training</a>	YES



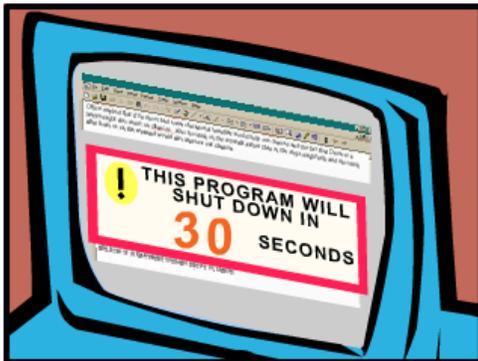
# Securing Remote Computers

Page 1 of 4

Click the links to learn more. Click Next to continue.

Audio | Back | Next | Exit

- 1. Introduction ✓
- 2. RA Basics ✓
- 3. Operating System Security ✓
- 4. Antivirus Software ✓
- 5. Personal Firewalls ✓
- 6. Social Engineering ✓
- 7. Personal Path to Security ✓
- 8. Certification Agreement ✓
- Print Certificate
- EXIT COURSE



Around the world, hundreds of thousands of unprepared systems were disabled by Blaster.

## The Threat is Real

Maria, a remote access user, was a victim of the Blaster worm. It caused her to suddenly and unexpectedly lose control of her computer and her work. It also passed into the NIH network through her remote access connection.

Blaster got Maria because she didn't have her system patches updated on her personal system, which she was using for NIH work.

Attacks like this one are attempted every day, but most can be avoided with the right security tools and practices in place.



# Securing Remote Computers

## NIH Remote Access User Certification Agreement

**Directions: You must scroll through this document and click on the "I Agree" button at the bottom of this page in order to record your acceptance.**

An employee, contractor, or other authorized user may be authorized by management to have remote access connectivity to NIH resources if there is a clear mission-related need.

1. All remote access connections and services that connect to NIH resources, whether furnished by the government or by the user, shall be used only by the individual authorized below and for authorized use only.
2. All authorized users who have been provided remote access to the NIH network must take annual NIH Computer Security Awareness Training at <http://irtsectraining.nih.gov>.
3. All authorized users shall ensure that resources remain secure from damage and unauthorized use in accordance with:
  - o NIH IT Security Policies, Standards and Procedures at [http://ocio.nih.gov/security/sec\\_policy.html](http://ocio.nih.gov/security/sec_policy.html) [link](#) in particular:
    1. The NIH IT General Rules of Behavior at <http://ocio.nih.gov/security/nihitrob.html> [link](#)
    2. The Limited Authorized Personal Use of NIH Information Technology Resources Policy at <http://www3.od.nih.gov/oma/manual/chapters/management/2306/> [link](#)
    3. The NIH Remote Access Policy at <http://oma.od.nih.gov/manual/chapters/management/2310/> [link](#)
    4. The NIH Remote Access Security Standards and Procedures at [http://ocio.nih.gov/nihsecurity/NIH\\_Remote\\_Access\\_Standards\\_FINAL\\_doc](http://ocio.nih.gov/nihsecurity/NIH_Remote_Access_Standards_FINAL_doc) [link](#)
  - o DHHS Cybersecurity Program Policies, Standards and Other Documents [http://intranet.hhs.gov/infosec/policies\\_type.html](http://intranet.hhs.gov/infosec/policies_type.html) [link](#)
  - o Local Institute/Center (IC) IT security and remote access policies. [Note: ICs may require authorized users to sign additional remote access user agreements with more stringent requirements].
4. Authorized users are also responsible for:
  - o Ensuring that systems are secure and that anti-virus software is installed, running, and updated regularly on all end user remote access systems prior to using them. Authorized users of NIH-provided software should obtain the software from <http://www.antisvirus.nih.gov/>
  - o Ensuring that they utilize, maintain, and store highly sensitive information on NIH network servers when feasible. Government data cannot be stored on personally-owned equipment.
  - o Reimbursing the government for any unauthorized use of government resources (by self or other individuals) or damages that result in charges to the IC that result from inappropriate use.
  - o Notifying their Administrative Officer and supervisor when remote access resources and services are no longer required to accomplish mission objectives.
5. NIH will review all remote access accounts (at least) annually to ensure that there is a continuing need for the remote access resources and privileges.

### NIH REMOTE AUTHORIZED USER CERTIFICATION AGREEMENT

I have read and understand the requirements stated above and agree to adhere to them for the duration of time I have NIH network remote access services. I understand that if I violate any of these standards and procedures, I may be subject to cancellation of my remote access privileges and/or disciplinary action.

I AGREE

Local intranet | Protected Mode: Off

100%