

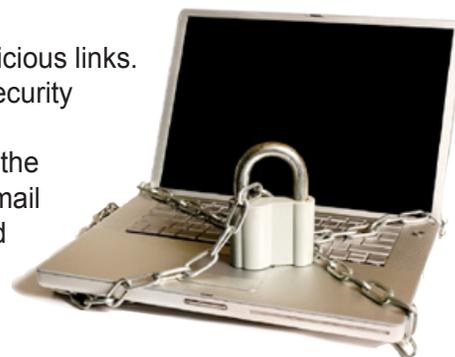
SecuritySmart

Protecting Your Computer

The Laboratory's Yellow network prevents most cyber attacks. Computer users are an integral part of Yellow network defenses and must ensure their own systems are protected.

Steps to Take

- Do not open unknown email attachments or click on suspicious links.
- Download and install the most recent operating system security patches.
- Ensure an anti-virus application is installed, updated with the latest definitions, and functioning to frequently scan (1) email for viruses, (2) all files being accessed by the system, and (3) all files on the system.



Passwords

Wherever possible, a token card (CRYPTOCard) that generates a one-time passcode should be used for authentication. When a token card cannot be used, creating strong passwords is important in preventing unauthorized access to your computer. Reusable passwords:

- must be a minimum of 8 characters and be changed at least every 180 days;
- must contain a variety of characters (upper-case letters, lower-case letters, numbers, and symbols);
- cannot be names or common words (those found in a dictionary); and
- must never be shared.

See Attachment A of Cyber Security Access Controls, P218 (<https://policy.lanl.gov/pods/policies.nsf/MainFrameset?ReadForm&DocNum=P218&FileName=P218.pdf>), for more information.

Traveling

Computers (usually laptops) that are taken on travel or used at home are generally more susceptible to being infected than computers that stay within the Yellow network. Some precautions to take:

- Before taking a system off site, ensure that it has the latest patches and anti-virus definitions. Laptops must be checked for viruses (using the latest anti-virus definitions) BEFORE they are re-connected to the Yellow network.
- All laptops taken on foreign travel must be borrowed from the Laboratory's laptop pool. There are property, export control, and security issues that must be addressed. Contact your Organizational Computer Security Representative (OCSR) for more information.

Reporting an Information Security Incident

Report all potential information security incidents to the Security Inquiry Team (SIT) at 505-665-3505. After hours or on weekends, page the On-call Duty Officer at 505-949-0156.

For more information, see the Security Smart on Computer User Responsibilities: http://int.lanl.gov/security/documents/security-smart/2009/comp_resp509.pdf

Resources

Information on anti-virus definitions is available at <https://esd.lanl.gov>

Send questions regarding network security to csirt@lanl.gov