

Best Practices

Technology in Schools

DRAFT

Users who access web-based e-mail with Community Net connected computers, Personal Digital Assistants (PDA's), cell phones and networks are to follow the guidelines below.

- Web-based e-mail account names **MUST** be different from division network account names.
- Web-based e-mail account passwords **MUST** not be the same as division passwords.
- Passwords should not be words found in the dictionary.
- Passwords should contain alpha and numeric characters and be at least 8 characters long.
- Browsers **MUST** be configured to prompt the user before external code is run.
- To avoid the inconvenience of logging in and out of web-based e-mail, some websites will ask if you wish to store your password in a browser cache or cookie. **DON'T DO THIS.** If you do, anyone who has access to your computer can access your account.
- **DON'T** configure web-based e-mail to automatically forward to work/school e-mail accounts (or vice versa).
- **DON'T** forward restricted or confidential e-mail to your web-based e-mail account.
- Most Web-based e-mail does not include encryption. Therefore, business information, information of a confidential or sensitive nature, such as credit card numbers, passwords and other personal information, should not be sent.
- **NEVER** open suspicious or unexpected e-mail attachments. They may contain a script or executable program that can delete local files, send files/documents or passwords to another host and severely damage the network.
- **DON'T** send large attachments.
- Always scan attachments with up-to-date virus software prior to opening.
- The subject line in e-mail should always be filled out.

It is unacceptable to send large attachments such as singing Christmas cards or animated Valentine's greetings as attachments to e-mail - such attachments can seriously affect the performance of Community Net's network. Remember that e-mail is the leading source of computer viruses, be especially suspicious of attachments. Unencrypted e-mail is not secure. Users have a responsibility to put only non-sensitive information in an e-mail, unless an agreement about confidentiality has been reached with the recipient in advance. The recipient is responsible for handling the message with respect and securing the sender's permission before forwarding it.

- Be extra cautious when reading e-mail - if you receive an email with a subject that seems "unusual" or "unexpected" and if the context of the message seems a bit odd, phone the Help Desk - let them check it out first and verify that it is in fact a legitimate e-mail.
- Never open (double-click) on an attachment that has an extension of .vbs, .exe or .bat - it is always better to first save the attachment, scan the file for viruses and then run it - and even at that be sure to verify with the person who sent the e-mail that he or she did in fact send it to you and that it is indeed legitimate.
- Never "assume" an e-mail message with an attachment is legitimate. Just because a message comes from your co-worker doesn't necessarily mean it is safe. That co-worker may have sent you an infected message - without even realizing it! If you are at all suspicious, it only takes a minute to confirm with the other person that the message is valid.
- Turn on file extensions.

Local Area Network Requirements:

- User group internal cabling structures must be certified to support the intended network standard, i.e: Ethernet will require structured Category 5 or better cabling, installed by certified professionals, and tested to meet or exceed Ethernet standards. Patch cables should be pre-fabricated, molded Category 5e or better. The same methodologies must apply to all user group Token Ring, ATM, and other network types.

- It is HIGHLY recommended that user groups segment their Ethernet based LAN's with VLAN's to ensure security of information traveling amongst separate user groups, i.e: Students/Teachers/Library/Office
- It is HIGHLY recommended that user groups install network equipment that will support access control lists, quality of service, port replication (SPAN), and multicast filtering technologies.
- User groups should implement some type of Intrusion Detection System (IDS) to provide early warning of attacks and logging and tracking facilities for attacks/issues. A good example of a free IDS utility is Snort.

It is the policy of the EDUVPN to ensure that people with hearing, visual and other disabilities have equal access to public information that is available on the Internet and the World Wide Web. It is the direct responsibility of the EDUVPN and its web page developers to become familiar with the guidelines for achieving universal accessibility and to apply these principles in designing and creating any official Website. The use of information technology should not create new barriers for people with disabilities. It should be used to reduce barriers and enhance accessibility.

Hosts for conferences will ensure strong user ID's and strong Passwords are used to for all sessions. Account ID's should be equal to or greater than 8 characters.

- Passwords should be a minimum of eight (8) characters in length.
- Passwords should also contain the following three character types:
 - An uppercase character (for example, C, M, Q)
 - A lowercase character (for example, a, g, t)
 - A number/special (for example, 1, \$, &, 4, 7, !).

Generic Accounts and Passwords are inappropriate.

The user will ensure strong encryption is used to help guarantee the confidentiality of the data transmitted.

Firewalls:

- Must meet the criteria specified by the ICSA Certification Process for modular small to medium business firewalls and should be ICSA certified to the latest revision (www.icsalabs.com).
- Must support the connection of the user group to Community Net, in terms of throughput and packets per second. Typically home network gateways such as D-Link or Linksys products will not meet these criteria.

Wireless:

-
- groups that use wireless technologies to connect their users to the EDU VPN must ensure that security is paramount when designing and installing systems.
- Encryption such as 128 Bit WEP must be used in conjunction with some type of 802.1x/RADIUS security methodology, a good example of this is EAP.
- Wireless networks must be secured such that only those users who have their Network Address specifically allowed within the access points are allowed to join the network.
- Wireless networks must be on some type of private service network that requires VPN access into the production network to allow usage.

Notebooks:

- When at the airport, never check a portable computer with luggage.
- When passing through security be aware of the location of the computer at all times, as portable computer thefts occur during the security process.
- Do not store written passwords or instructions on how to logon to networks with portable computers.
- Always transfer confidential information off the portable computer if the computer is shared by others.
- File encryption software must be used for confidential information stored on the notebook