INTERNET ORIENTATION

NETIQUETTE

The purpose of this orientation is to provide users with some starting guidelines for acceptable use of the Internet via State equipment. We all know that information technology is exploding at a rate much faster than can be matched by the formal policies and procedures, which are supposed to govern and control its use. Our goal is to expose Internet users to Internet etiquette and useful concepts, and to provide fair warnings that should ensure that state employees continued to have access to this rich information resource.

DOWNLOADING FILES

File Types

The Internet is an unimaginably vast source of files that can be copied to your PC, or “downloaded.” These can be divided into two broad catagories: data files and executable files.

Data Files

Data files are made up of words, numbers, pictures, sounds, or even full-motion video images. This is raw digital information which has been created and stored using some application program.

The primary concern that users should have regarding data files is the awareness that you can quickly consume large quantities of disk space.

In order to encourage reasonable space usage on the Administrative Services network, we are recommending that downloaded data files be stored on the user’s local hard disk (drive C:) or on floppy disks, rather than on the network. Network storage not only consumes disk space shared by others, but also involves more overhead for network backups. You will want to check with your own network administrators for the preference or policy on storage of downloaded files.

Executable Files

Executable files, often referred to as “applications” are programs that *do* something. Once downloaded to your PC, your operating system can execute these files. In addition to the previously mentioned storage concerns, these files have several inherent dangers, and are a significant concern.

Installation and Configuration Issues

When you download executable software, part of the process of installation – whether manual or automatic – is usually to make modifications to your current PC configuration. In a typical Windows "setup" program, files are copied into the Windows system directory, and several workstation configuration files are modified. It is therefore important to note that installation of new software may cause other pre-existing business software to fail. Please don't expect your network support technicians to remedy problems caused by the installation of unsupported software.

Viruses

Definition: Computer viruses are analogous to their biological counterpart. These programs invisibly attach themselves to other executable files or to the operating system, and are capable of self-replication. During their replication phase, infected programs appear to run normally, the goal being to quietly infect other application programs and spread to other workstations. Once a virus is triggered, typically by reaching a predetermined target date or by having performed a certain number of replications, it enters an active state. At this point a virus has no further need for concealment, so many viruses are detected only at this point. The goal of the active virus may be benign – printing a message of universal love on the screen – or it may corrupt or delete all data files to which you have access.

Obviously the destructive potential is much more serious on a network than for a stand-alone user, since a virus has the same access rights as the network user. If you have permission to modify the files created by others in your division, for example, a virus on your machine puts all of your group's data at risk.

According to current literature there are somewhere on the order of 5,000 different types of computer viruses currently in circulation, with that number increasing by over one-hundred per month.

Until recently, the most common vector for viral infection at work was software carried from home or downloaded via modem. Access to the Internet means that you have the potential to pick up suspect software from all over the globe without leaving your desk.

Don't Panic!

Very rarely is a computer problem related to a virus. So don't panic! When a computer has a problem, there a hundred more probable causes.

Virus scanning software is available commercially, and all network administrators should have current software. Because of the proliferation of viral types, this software should be updated frequently. It is a good policy to scan any new executable file once before allowing it to be run on an office machine.

Abstinence: The only way to get a virus is to run an infected program. If you run only commercial "shrink wrapped" software, viruses are the least of your worries.

Thinking the Unthinkable

Even if you do discover a computer virus, very few users have the ability to modify network applications – and data files do not carry viruses – so the spread of infections is limited to people with whom you have exchanged application software. It will be up to you and your network administrator to detect and eradicate infected programs using anti-virus software and backup copies of the infected applications.

Software Policy and Legality for Files of All Types

External Considerations

> ***Users need to be aware that there is no central governing body on the Internet. Therefore no censorship or licensing control exists except that which you exercise on your own. If you spend much time on the Internet, you will eventually come across information that is illegal or proprietary. For your own protection, you should be aware that downloading – and therefore possession – of such information may have legal ramifications, both professionally and personally.***

Licensing Violations

Commercial software is sometimes distributed illegally via the Internet, where it is downloadable for any user worldwide.

Copyright Infringement

Commercial photographs, music, documents, and other forms of proprietary information are available for downloading.

Internal Considerations

Within Administrative Services, the current policy on the introduction of new software states that employees must (a) have the permission of their supervisor before installation, and (b) they must keep some proof of legal software license or registration at the workstation where the software is installed.

The goal is to ensure that supervisors are kept aware of what software is used by their employees, and to ensure that each division fully complies with its legal obligations. (Responsibility for standard network software is in the domain of the network administrator.)

You may want to check with your supervisor on your own internal software policies.

INTERNET SECURITY

Internet email is *not* secure

Mail traverses the Internet using the best available route, chosen second-by-second by the network hardware. You don't know whose network your data crosses and, given the right equipment, anyone along the route can read your messages. Consider Internet email messages public, and write them accordingly.

If you have statutory or personal security requirements, see your network administrator about ways to password-encrypt your mail before you send it.

Internet Transactions Aren’t Secure, Either

There is currently no generally-accepted method for the secure exchange of monetary transactions or data. This area is a hotbed of activity, at present, and is expected to change in the near future. For now, however, if you are prompted to supply credit-card, internal business, or personal information over the Internet, defer to a phone call or some medium of exchange that can’t be monitored.

Assume that any Internet activity can be monitored – and be able to defend your business usage.

Administrative Services is currently monitoring all of our own Internet traffic in order to establish base-line data on usage trends how much load we can support. As a side-effect, the activity between any individual workstation and the Internet can be examined in detail.

The Department of Administration is presumably doing the same thing with all State of Alaska Internet traffic.

We don’t police the network! However, when you connect to an Internet site, anyone attached to the wires between you and that host could do so – and could tell your boss how much time you spend reading Internet comics.

Think About Your Own Network Security

Now that our Wide Area Network is part of the global Internet, your network administrator may be more serious about security than in the past. Do your part by ensuring that your network passwords are kept private, are changed whenever potentially compromised, and cannot be easily guessed.

BANDWIDTH

Definition of Terms:

“Bandwidth” is a term describing the rate at which a given amount of data can pass through a network cable. You will also hear this described as the “size of the pipe” down which signals move. All employees of the State of Alaska get access to the Internet using a common “56-Kilobit” pipe. This means we share a bandwidth of 56,000 bits of information per second.

Significance

Receiving 200K of data over the Internet ties up the pipe for the entire state government for a period of about twenty seconds, under ideal conditions. More realistically, this figure could reach twice that, or forty seconds. Pulling 200K of information down the pipe is not that unusual when visiting a remote site, and there are a large number of other users also wanting their chunks of time. A responsible Internet citizen doesn't tie up the Internet during working hours for frivolous purposes.

PHYSICAL LOCATION

Be aware of where information your information comes from...

The Internet is a world-wide resource made up of interconnecting networks, and it is not always readily evident when you are receiving information from a location outside of the North American continent. While some areas have multiple connections going in many directions, there are still a limited number of intercontinental pipes going overseas. This means that, on intercontinental connections, you are sharing resources not just with the State of Alaska government population, but literally with the world. The Internet is there to be used, but Netiquette suggests that a user does not frivolously transfer large amounts of data across international boundaries.

Due to this bottleneck, some popular sites have scattered "mirror" sites with identical information to allow users to find information locally, without contending for the overseas lines. Look for the information nearest you, if possible.

...and what the local time is there.

Intercontinental connections are especially critical during peak load hours. Many businesses and universities depend upon limited intercontinental connections during their local daylight hours. 10:00 a.m. in Juneau, for example, is 4:00 a.m. in Tokyo, which should be relatively quiet. 3:30 p.m. here, however, is 9:30 a.m. there – by which time traffic will be considerably worse. If you take advantage of off-peak hours everyone gets faster response time.

How can I tell where information is coming from?

Most Internet resources are pointed at by a URL (Unambiguous Resource Locator), a short series of characters formed in a hierarchy, separated by periods. The URL for one Administrative Services site, for instance, is "health.hss.state.ak.us". The significant thing to note here is that the last part of this URL is "us". This implies that this is a location in the United States. Other designations associated with the United States are "gov" (government), "net" or "com" (commercial site), "mil" (military), and "edu" (educational site).

On the other hand, if the URL ends in "ca", it is from Canada. If it ends in "de" it is from Deutchland (Germany). "uk" is England (Great Britain) and "au" is

Australia. Many Internet texts include an appendix with a listing of these suffixes.

For the most part, it is sufficient to realize that if the suffix you are accessing is not “us”, “gov”, “mil”, “net”, “com” , or “edu”, you are accessing an international site, and you should examine the necessity of your network traffic. Again, the Internet is there to be used, but you are sharing it with millions of other users, many of whom are depending on it to complete their research or correspond with their colleagues.

TIME USAGE

Use, particularly learning, of the Internet can be a tremendous time sink.

Be aware, both for yourself and for those you supervise, that the Internet can subtly consume great quantities of time.

PLAY

If you want to play with the Internet there are reasonably priced vendors offering access that doesn’t burden state resources.

The IS staff has the names of a couple of vendors that will provide access for all of those terrific sites you’d love to explore but can’t justify doing on State time and equipment. If you own a PC and a modem – and a little ready cash – the world can be yours.