

Safe E-mail Practices

The BC Government has spent considerable effort and resources to make our Shared Government E-mail System (Exchange) robust and secure. These safeguards consist of layers of firewalls, anti-virus software and filtering mechanisms designed to prevent known threats from getting into Government's IT infra-structure. If a computer virus gets past these layers, additional protections prevent the propagation of a known infection from one desktop to another.

These safeguards, like any immune system, are continually challenged by new viruses and attempts to intrude into the infrastructure. To date, the BC Government has not succumbed to a major e-mail virus attack or a denial of service attack such as other organizations have experienced and that we read about in the press. The BC Government's Virus Emergency Response Team (VERT) has worked well in monitoring and responding to threats.

Safe E-mail practices are needed to ensure that computer viruses in the BC Government do not become an epidemic. These safe practices consist of:

- ◆ Support the efforts of your ministry VERT coordinator.
- ◆ Heed the warnings from your VERT coordinator and immediately take their recommended action.
- ◆ Ensure anti-virus software on your government workstation is kept up-to-date.
- ◆ Do not access non-government e-mail systems from a government workstation. ***Accessing these e-mail accounts on the Internet opens a backdoor to the PC and circumvents the safeguards surrounding government e-mail systems.***
- ◆ Do not permit any non-government network connection to government workstations (no dial modems, no ISP Internet connections).
- ◆ Look for and recognize suspicious e-mail attachments and do not open them.
- ◆ Always 'save' e-mail attachments first, and then open them. This ensures they will be scanned by anti-virus software.
- ◆ When accessing government e-mail systems from home, do the following:
 - ◆ Use government approved access methods (Span/Dial, "Snow", VPN, Microsoft Windows Terminal Server, 128-bit Secure Sockets Layer)
 - ◆ Use strong passwords which are changed monthly
 - ◆ Use anti-virus software and update virus signature files regularly (weekly)
 - ◆ Use a personal firewall on all home Workstations
 - ◆ Turn off Microsoft Windows sharing options
 - ◆ Update manufacturer software with security fixes regularly
 - ◆ Disconnect VPN connections to governments network and turn off the computer when not in use

These safe practices will ensure we continue to have an enviable record of e-mail system availability.