

Guard your computer systems against attacks

Keep your computer systems secure by evaluating your security practices regularly and by performing a security audit at least twice a year - when you're focused on changing your clocks. The Better Business Bureau with the cooperation of the Federal Trade Commission and the National Cyber Security Alliance have developed a checklist to help businesses guard their computer systems against attacks.

"Computer security is a critically important issue that can impact any size business with a computer and Internet access," said Ken Hunter, president and CEO of the Council of Better Business Bureaus. "Our checklist provides an easy-to-read, easy-to-use tool that will hopefully encourage more business owners and managers to take steps to guard their computer systems against intruders."

"Large and small businesses need to take computer security seriously. This handy checklist should make it easier to do," said Howard Beales, Director of the FTC's Bureau of Consumer Protection. "Consumers also can adopt the checklist to protect the information on their home computers." The checklist recommends:

- Maintain a password protection program.** Use cryptic phrases that combine numbers and both upper- and lower-case letters instead of a "simple" password. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "I love Felix; he's a good cat," would become 1lfha6c. Your system should require all users authorized to access your network to create a password when they first log in, change it regularly (at least every 90 days), and lock out prospective users who fail to enter the correct password three times in a row.
- Use virus protection software.** Install virus protection software on all your computers, and check back routinely with the provider for updates. Most anti-virus software can be set up to update itself weekly. Scan your systems for viruses continually, and never disable anti-virus software.
- Install firewalls.** Equip your computers with firewalls, which are available wherever software is sold. Firewalls are gatekeepers; they protect a computer network by shutting out unauthorized users and admitting others only to the areas they are authorized to access. Install firewalls at every point where your computer system is connected to other networks, including the Internet, a separate local area network (LAN) at a customer's site, or a telephone company switch. Firewalls should be set up to prohibit all activity except what is required to operate your business.
- Use security patches.** Most software vendors release updates and patches to their software to correct "bugs" that might allow entry to your computer. Check your software vendors' Web sites for new security patches; download and install them routinely. Easier still, use the new automated patching features that perform these tasks.
- Back up your data.** Set an example for your staff by backing up the data on your computer weekly, at a minimum. Back up small amounts of data on floppy disks; use CDs to back up more. Keep these disks in a secure place. If you have access to a network, save copies of your data to another computer on the network.

- **Routinely check for suspicious activity.** Almost all firewalls, encryption programs, and password schemes include an auditing function that records activities on the network. Check data logs and audit trails for unusual or suspicious activity.
- **Note the risks of file-sharing.** Your computer operating system may allow other computers on a network, including the Internet, to access your computer's hard drive to share files. File-sharing can lead to viruses, as well as a competitor's ability to read the files on your computer. Unless there's a business reason to share files, consider turning off this function and prohibiting your employees from installing file-sharing programs on their computers.
- **Consider buying encryption software.** Even if an intruder manages to break through your firewall, the data on your network can be secure if it is encrypted. Stand-alone encryption packages that work with individual applications are in the public domain and available for sale.
- **Educate your employees.** Develop and enforce a company-wide computer and physical security policy that tells employees:
 - Not to open email from sources they don't know
 - What to do when they receive suspicious emails (when in doubt, delete)
 - To disconnect from the Internet when they're not using it;
 - The risks of file-sharing;
 - How to perform back-up procedures; and
 - What to do if their computer becomes infected

Copies of the brochure, "Is Your Business Cyber Secure" are available from the FTC's Web site at <http://www.ftc.gov> and also from the FTC's Consumer Response Center, Room 130, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on any of 150 consumer topics, call toll-free, 1-877-FTC-HELP (1 877-382-4357), or use the complaint form at <http://www.ftc.gov>.