

Risk Alert



Listening. Learning. Leading.®

Hackers attack an innocent victim every 39 seconds

According to a study completed by the Institute of Electrical and Electronics Engineers (IEEE), a hacker attacks a different computer every 39 seconds. That's 2,244 attacks every day—2,244 times that someone attempts to steal information, alter computer files or commit other cyber crimes through another person's system.

How does this affect religious institutions? Computers at worship centers commonly contain valuable data, such as financial records, personal information and irreplaceable documents—all very attractive to a cyber criminal. Utilize cyber security in all of your computer-related practices to protect these electronic valuables.



What needs to be protected?

Determine what information is most imperative to the security of your organization by conducting an information audit of electronic files. Take an inventory of all computers, tablets, smartphones, flash drives, disks and electronic storage devices that are used for business purposes and the information that each contains. Make sure that all financial information about your organization, information about members of your congregation, employee information and other "private" documents are stored on a computer without Internet access. Review the rest of the information you gather and determine if it is necessary to have. If the information is not needed, properly dispose of it.

Destroy unneeded paper records, credit cards and disks using a quality, crosscut shredder. Even more precaution is required when disposing of records on your hard drive. Simply deleting them is not enough. Invest in a wipe utility program that will overwrite your hard drive or use a company that specializes in computer equipment and file disposal to adequately erase your unneeded records.

Security for the cyber world: how you can feel safe

After you have determined what you need to protect, implement cyber security to guard your organization's computers against attacks from the different types of malicious software or "malware," such as viruses, worms, Trojan horses, phishing and many other types of system corruption.

For basic protection from malware, there are a number of software programs that you can install on your system. They are available for purchase online and at many retailers. Minimally, your computer should have an anti-virus and anti-spyware program, a firewall and operating system updates installed on its system and updated regularly.

(Over)

Is your computer infected?

Even after you've taken all the precautions, a hacker could still find a way to get into your computer system. Some signs that your device may be infected are:

- The system slows down, malfunctions or displays repeated error messages.
- The system won't shut down or restart.
- The system displays an unusually large number of pop-up ads, or they come up when you're not surfing the Web.
- The system displays Web pages or programs you didn't intend to use or sends email you didn't write.

Taking a stand against intruders

If your device shows symptoms of being infected, stop intruders in their tracks by:

- Confirming that your security software is active and up to date.
- Running your computer's security software to scan for viruses and spyware and deleting anything that the program identifies as a problem.
- Stopping any banking, shopping or other online activities that involve user names, passwords or other sensitive information until you are absolutely sure that your computer is not infected.

If you suspect that your computer is still infected, run a second anti-virus or anti-spyware program or contact a professional for assistance. In the meantime, try to determine how the malware could have been downloaded to your machine and what you can do to avoid it in the future.

Seven steps to safer computing

Practice these simple habits in your computer, tablet and smartphone use to reduce the risk of a malware invasion on your system:

1. Protect personal information. A name, Social Security number and date of birth are all that a criminal needs to steal someone's identity.
2. Always know whom you're dealing with.
3. Use anti-virus software, anti-spyware software and a firewall and update them regularly.
4. Check the security features on your operating system and Web browser to make sure they are adequately protecting you. Update these features and the browser software regularly.
5. Protect your passwords by keeping them in a secure place that's out of plain view and by never sharing them over the Internet, telephone or email. Don't use common words, personal information, your log-in name or the same password from other accounts when creating a password. Instead, create a long password with symbols, numbers and letters and change it at least every 90 days.
6. Periodically back up important files to a network, external hard drive or other device.
7. Find out whom to contact if your computer gets hacked or infected (i.e., your Internet service provider).

To learn more about cyber security, visit www.us-cert.gov/cas/tips.

For a complete collection of the *Risk Alert* series, visit our website and look in the Safety Resources section.