Cybersecurity: Everyone's Responsibility

At-A-Glance

What's happening in cyberspace?

A recent survey of governments, businesses, and individuals in the U.S., China, Russia, and India found that more than 88% of respondents believe that cyberspace threats are significant. While many respondents feel comfortable with online banking and shopping, more than 69% are not comfortable with sharing identity and personal data online.

This is a valid concern—the latest Internet Crime Report by the Internet Crime Complaint Center shows an increase in cyber crimes, as thieves seek out personal data and other valuable information for their own advantage.

> "At Cisco, we're seeing many signs that criminals are mimicking the practices embraced by successful, legitimate businesses to reap revenue and grow their enterprises. It seems the best practices espoused by *Fortune* magazine and Harvard Business School have found their way into the online underworld."
>
> Marie Hattar
> VP, Borderless Networks Marketing, Cisco

Why is cybersecurity important?

Cybersecurity is a necessary consideration for individuals and families, as well as businesses, governments, and educational institutions.

For families and parents, online safety of children and family members is of paramount importance. In terms of our financial security, It's critical to protect information that could impact our personal finances. And, by protecting our computers, we protect precious family assets such as photos, as well as videos and music.

For faculty, staff, and students, the Internet has provided huge learning opportunities as well as risks. Students, teachers, and administrators need to understand how to protect themselves, and must understand the link between the online and "real" world. Learning how to protect computers and engage in appropriate online behavior will reduce vulnerabilities and create a safer online environment.

Small and medium-sized businesses face critical challenges due to limited resources and information, as well as competing priorities. The speed at which technology is evolving makes it difficult to stay current with security. However, better security awareness and planning can help these businesses protect their intellectual property and trade secrets, and reduce loss of productivity due to downtime.

Local, state, and central governments maintain an enormous amount of personal data and records on their citizens, as well as confidential government information, making them frequent targets. Yet many government entities are challenged with insufficiently secured infrastructure, lack of awareness, and competing funding and resource priorities. Better security helps government bodies provide reliable services to the public, maintain citizen-to-government communications, and protect sensitive information.

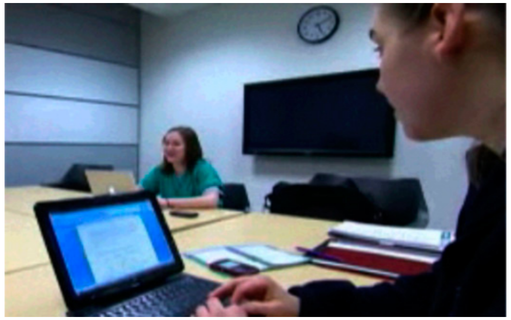
What is my role in cybersecurity?

It's important to recognize the different types of risks that exist in the online world. When online, keep this in mind: Stop. Think. Connect. Stop for a moment. Think about how you will take care of your information and personal data before acting. Connect responsibly. Following are some descriptions of risks, and some actions you can take.

Phishing: Phishing uses email or malicious websites to solicit personal or financial information. This can take the form of an email, seemingly from a reputable credit card company or financial institution, that requests account information. When users respond with the requested information, fraudsters can use it to gain access to the accounts. **Do not open messages or attachments from unknown sources**. Use spam filters to prevent unwanted and dangerous email.

Spyware: The two important things to know about spyware programs are that 1) they can download themselves onto your computer without your permission when you visit an unsafe website and 2) they can take control of your computer. Keep your computer up to date—especially your operating system, web browsers, and antivirus/antispyware protection.

Safeguard Open Academic Network



Baylor College of Medicine, a premier academic, research and clinical facility, employs Cisco solutions to protect sensitive data on the network.

Password protection: Choose strong passwords that are not easy to guess. Avoid your address, pet's name, or a child's name. Think of creating a password by using the first letter of each word of a favorite saying. Substituting capital letters and/or numbers for some of those letters will strengthen the passwords even further. Make sure to change your passwords regularly.

Social media: Although social media can be a fun experience and can help you stay connected, it can also create an opportunity for information leakage or even compromise personal identity and safety. Be smart with your identity on social media sites. Make sure to review and use privacy settings. Keep all tagged photos private. Do not share information that can help people steal your personal identity.

Plan ahead: Prepare for worst-case scenarios. Keep copies of family photos. Review financial and personal credit records on a regular basis. Back up critical data. Have a fall-back plan for businesses, schools, and government bodies.

Where can I find additional resources?

The National Cyber Security Alliance has more tips and cybersecurity awareness information. Visit http://www.cisco.com for cybersecurity awareness information and solutions for families, education, small businesses, and governments.