Protect your personal information from online risks

Going online has become part of everyday life – whether for shopping, sending email or paying bills and managing accounts. However, many worry that technology-related issues, including unsolicited emails and unsecure websites, can affect information stored online. The 2013 Travelers Consumer Risk Index shows that 41 percent of Americans worry about computer and technology issues. These were ranked second among the top five risks causing the most concern. View the infographic. Taking precautions when browsing the Web can help reduce your risk of a cyber attack. Read these tips to learn how to help stay safe online.

Online shopping

- You should research retailers to make sure they are reputable and have a secure network and website. Avoid buying from a site that does not have a secure socket layer (SSL) encryption installed. Look for the 's' at the beginning of a URL – HTTPS:// instead of HTTP:// – to help determine if a site is SSL secured.
- Read the site's privacy policy to learn how the personal information you provide will be used.
- Use only one credit card for online purchases. Be sure to open statements when received to check for fraudulent charges or activity.
- If you receive an email regarding sales or discounts from a particular retailer, log on directly to the official website for the business. Avoid linking to it from an unsolicited email.

Emails and attachments

- Do not send personal information in email or instant messages. Emails are out of your control once sent, and can be easily intercepted.
- Only open attachments from senders you know and trust. If unsure, you can run a virus scan on attachments before opening.
- Do not download files or programs or click on links from senders you do not know and trust. Consider whether to open emails from retailers if you know you are not on their email list. If you are unsure if an email came from a trusted source, hover over the link to see where it leads.
- If you receive unsolicited spam email, do not respond or click on any links in the email.
- Be cautious of emails you receive regarding your financial accounts. If you are not sure of the email's validity, contact your financial institution directly.

General online safety

- Limit personal information you put on the Internet. Social media sites can be good for networking, but identity thieves can use the information you share.
- Keep your Web browser up to date. This can help ensure the latest security features are installed.
- Avoid storing personal information, account numbers and personal identification numbers on your computer.
- Install firewall and anti-virus software. This can help protect you from exposure to malicious cyber attacks.
- Choose strong passwords and keep them private.