



STOP | THINK | CONNECT™



PROTECT YOUR CUSTOMERS

Trust is an essential element of customer relationships. When it comes to Internet security, your customers trust you to protect the personal information they share with you. You would never knowingly put them at risk, but lax computer security practices can do just that – jeopardize your customers’ sensitive information and expose them to threats. If your company has a website, communicates with customers via email, or stores customer information in an electronic database, you could be putting them at risk if you aren’t taking the right precautions. Following a few simple online safety practices can protect you from incurring expensive and dangerous data breaches, and give your customers the peace of mind they deserve.

GAIN THEIR TRUST

The following information practices will help safeguard your customers’ data and help them feel confident about doing business with you online.

Have (and follow) a privacy policy

Your company’s website should have a privacy policy that tells customers what information you collect and how you use it.

Know what you have

You should be aware of all the personal information you have about your customers, where you’re storing it, how you are using it, who has access to it and how you protect it.

Keep what you need and delete what you don’t

While it’s tempting to keep information for future use, the less you collect and store, the less opportunity there is for something to go wrong.

Protect what they give you

If you’re holding onto information about your customers, you need to keep it secure.

SBA’s participation in this cosponsored activity is not an endorsement of the views, opinions, products or services of any cosponsor or other person or entity. All SBA programs and services are extended to the public on a nondiscriminatory basis. Cosponsorship Authorization #16-3010-67 & #16-3010-99.

STOPTHINKCONNECT.ORG



@STOPTHNKCONNECT



STOPTHINKCONNECT



STOPTHINKCONNECT

PROTECT YOUR CUSTOMERS

BEST PRACTICES

Keeping your customers safe requires your own computer systems to be fully protected. The best policies in the world won't protect your customers if your network and resources are at risks for preventable attacks. Protecting your network and systems requires a lot of the same steps as protecting a single computer, only on a larger scale.

Keep a clean machine

Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.

Automate software updates

Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.

Scan all new devices

Be sure to scan all USB and other devices before they are attached to the network.

Use a firewall

A good firewall keeps criminals out and sensitive data in.

Use spam filters

Spam can carry malicious software and phishing scams, some aimed directly at businesses. A good spam filter will block most of it and will make your email system safer and easier to use.

Show your commitment to security

Participate in activities such as National Cyber Security Awareness Month and Data Privacy Day to demonstrate your business' commitment to security.

SBA's participation in this cosponsored activity is not an endorsement of the views, opinions, products or services of any cosponsor or other person or entity. All SBA programs and services are extended to the public on a nondiscriminatory basis. Cosponsorship Authorization #16-3010-67 & #16-3010-99.

STOPTHINKCONNECT.ORG

