Best Practices For Protecting Online Privacy

TREYSTA
technology management

The Internet can be a great tool for sharing information, connecting with new people, and accessing products and services you wouldn't be able to otherwise – but only if you (and those you care about) know how to do so safely.

The Inherent Risks Of The Digital World

Modern technology such as the cloud and mobile devices have made everyday tasks a simple matter for consumers. Unfortunately, when it comes to technology, greater convenience often comes with greater risk.

As the rate of adoption of new technology rises around the globe, so does cybercrime. It's more important than ever to ensure that you and your team practice safety when using technology in order to avoid identity theft, data loss, and other consequences.

At the end of the day, security comes down to you: the user. No matter what kind of firewalls, antivirus or other IT security software you or your team uses, if you're not being safe, you won't stay safe for long.

4 Types of Risks To Online Privacy

What are some of the risks to our personal safety online?

1. **Content:** All of you know the saying from reading the newspaper or watching TV that "just because it's in the news doesn't mean it's all true". Well, this same adage applies online because these days, anyone with an Internet connection can be a "citizen journalist" through blogs and social networks.

2. **Contact:** These are risks we're exposed to through our interactions online:

   a. Cyberbullying, which is using the Internet for repeated unwanted or cruel behavior against someone, opens the door to 24-hour harassment. Anyone can experience online bullying, but it's of particular concern among children

   b. Cyber harassment is the adult equivalent of cyberbullying.

   c. Child predators can also make unwanted contact with children. Although there is no doubt that this is the worst kind of contact (and makes the news most often), it's also the most infrequent form.

3. **Conduct:** The risks of conduct have to do with what we do and say online as well as what others post about us. Our reputations (and how others view us) are shaped by our actions, interactions, and what we post on social networks, in games and virtual worlds, or on mobile phones.

4. **Commerce:** Information about us, particularly about our online preferences and habits, is a valuable commodity to people and businesses, whether trustworthy or not.

   So the risks of e-commerce have to do with an invasion of privacy or identity theft when unsavory people get access to sensitive, personal information like bank accounts, credit card, or social security numbers.

Best Practices For Protecting Your Privacy Online

With all these risks out there threatening the user's safety, what can you do to protect yourself, your family, and your staff?

- **Defend Your Computer:** Cybercriminals work relentlessly to seize control of your computer, spread spam, or spy on your online activities — ultimately in an attempt to steal personal information or money.

  Criminals use two broad strategies to try to break through a computer's defenses:

  - They install malicious software on computers that haven't been updated. This can happen in a couple of ways. They can exploit older weaknesses in the software, or they can break into accounts guarded by simple passwords

  - They also try to trick people into installing their malware, including adware, worms, and key- stroke loggers (software that can spy on what you type—passwords, usernames, and so on).

In order to protect your computer (and anyone using it) against these cybercriminals, make sure to follow these two tips:

- Strengthen Your Computer's Defenses: Be sure to leave your firewall turned on at all times, as well as install robust antivirus and antispyware solutions (such as those offered by Microsoft® Security Essentials).

  Be sure to keep these solutions regularly updated and patched — it's as easy as setting them to auto-update, and clicking "Update" whenever prompted.

- Train Yourself To Act Cautiously To Avoid Downloading Malware: It's all about thinking before you click something — never download a file, whether online or as an attachment from an email if you're unsure of the source. It's always better to check with the sender to confirm, prior to downloading or opening a suspect file.

- **Protect Sensitive Information:** Your sensitive information — passwords, SIN, birth date, mother's maiden name, etc. — is valuable to cybercriminals, and they work hard to get their hands on it. Don't make it any easier for them.

  - Only use web pages with URLs that begin with "https" – if it's missing that "s", then it's not secure.

  - Save your online banking for home — don't perform any sensitive financial transactions on free, public wi-fi, where it's easier for hackers to gain access.

  - Avoid scams — don't fall for emails that want your information and have the following characteristics:

    - Generic salutations ("Dear Account Holder")
    - Sender email addresses that don't correspond to the organization they're speaking on behalf of
    - Alarmist tone, or a sense of urgency
    - Misspellings, poor grammar, and typos

- **Create Strong Passwords And Keep Them Secret:** The sad fact is that the most commonly used password worldwide is "password". You can do better.

  - To make passwords strong, use long phrases or sentences that mix capital and lowercase letters, numbers, and symbols.

  - Start with something like "Strong passwords are safer". With a little tinkering, you can come up with a password that is very strong and yet memorable, like this one: Str0ngpassw0rdsRsafer!

  - Don't use the same password everywhere. If it's stolen or inadequately protected by the site, all the accounts it protects are at risk.

  - Don't share your passwords with anyone or be tricked into giving them away. Many account takeovers occur because the owner disclosed the password.

- **Take Charge Of Your Online Reputation:** Given how quickly social media platforms rise, fall and change, you'd be surprised how much about you is out there. That's not to mention news stories, school information, and other content that may have been published about you years ago.

  Are you sure it paints the right picture?

  - **Discover What Is On The Internet About You.** Use multiple search engines and all variations of your name. Search for images as well as text. Review what others have posted about you in comments, pictures, or videos. Explore blogs, personal pages on social networks, and photo sharing sites.

  - **Then Evaluate The Story That Information Tells.** Because information online is searchable, often permanent, and may be seen by anyone on the Internet, ask yourself some questions. Your answers are important — they may determine what personal information you decide to share.

    Ask yourself these questions:

    - Does it reflect the reputation you want to have?
    - Is it accurate? If not, what should be deleted or corrected?
    - Do you need more than one online profile — whether professional, personal, or for an area of interest, like a hobby or volunteer work?
    - If so, is it okay to mix info from different profiles?
    - If so, what is okay to mix?

  - **Next, Take Steps To Protect Your Reputation.** Think about what you are posting and how it will reflect on your reputation. Talk with friends about what you do and do not want shared. Ask them to remove anything you don't want disclosed.

  - **Cultivate Your Reputation.** Be proactive about sharing the positive things you do online. For example, link anything you publish to your name. If you find information about yourself that doesn't fit the reputation you want to uphold, take steps to restore your online reputation.

    In a respectful way, ask the person who posted it to remove it or correct an error. If the person doesn't respond or refuses to help, ask the site administrator to remove the digital damage.

➤ Use Social Media Networks More Safely

- **Use Settings or Options features to help you:**
  - Manage who can view your profile and how public or private you want your profile to be.
  - Control how people can search for you—for example, by high school, current town, or employer.
  - Block any unwanted access.
  - As your preferences change over time, check those settings and modify them as needed.
- **Be selective about accepting new friends.**
  - Don't accept requests from people you don't know. Think before accepting colleagues or acquaintances, too.
  - Periodically reassess who has access to your account. Friends can change over time.
  - Review what your friends write about you. Make sure they don't share sensitive information. It's okay to ask someone to remove anything that you don't want disclosed.
- **Think Before You Post Something Online.** Remember that what you post may be seen by anyone and once it is out there, it's probably out there for good. So be sure to:
  - Keep details that could be used to identify you or your location—home address, phone, account numbers, etc. — private.
  - Never share your whereabouts. For example, wait to share vacation details until after you come back. No one needs to know that you are not at your house at a specific time.
  - Pay attention to what you post about others (including pictures), being careful not to share their sensitive personal information.

Don’t Undervalue Your Digital Privacy

With the rate at which technology is constantly evolving, it's important to take advantage of the latest tools available to you. When it comes to sensitive data, there’s no precaution too great.

Investing a little time and effort in best practices for online security now will help you avoid a number of risks and pitfalls in the future. Whether it’s just for yourself, or for your family and friends, staying safe online can save you a lot of stress and trouble.

If you need expert assistance implementing and managing safe digital practices at your place of business, the TREYSTA Technology Management team is available to help.

TREYSTA
technology management

(888) 242-0244 | www.teamtreysta.com