

12 Tips to Being Safer Online

This Safer Internet Guide is designed for nonprofits, charities, and NGOs.

You rely on the goodwill of your donors, constituents, and community for support. So it's very important that you protect your data and infrastructure. This guide is intended to help you keep it safe.

Our 12 tips include four main areas

At your office



There are some basic things that you and your staff should think about when you work in your office. Learn them before it's too late.

Use social media safely



Social media sites are the most visited ones online. Be aware of some dos and don'ts when you use them, both personally and professionally.

Away from your office



Most employees use multiple devices (such as laptops, mobile phones, and tablets) and use them in public areas. Consider these useful tips when you're away from your office.

Use the cloud safely



Online applications store your data on the Internet. These tips help ensure your data remains safe and uncompromised.



1 Make it more difficult for hackers

Be smart about passwords. After the physical security of your office, passwords are the next most important thing to consider. Use strong passwords with a combination of uppercase and lowercase characters, numbers, and symbols. This will help you defend against hackers who make random and systematic guesses that are based on commonly used words.

- Use different passwords for different websites. Use password management software to help you remember them.
- To thwart unauthorized password recovery that's based on commonly known information (your date of birth, the model of your first car, or your pet's name), consider whether you can use related but nonsense answers. For example, you could use the city in which a child was born, the model of your neighbor's car, or the color of your pet instead.
- Use two-factor authentication whenever possible. Two-factor authorization requires you to enter a code provided to you via either text message, a code generator app, or a security token device, in addition to entering a password.

Update your software. Hackers exploit vulnerabilities that are found in commonly used software such as your operating system, office productivity software, and web browsers. To prevent this, you should

- Install all updates to your software programs, and set them to automatically update, if that's possible.
- Install anti-malware software on all computers. If you have multiple networked computers, use software that provides enterprise-level security and that manages updates.

Block spam. It's essential to have a good spam blocker. Spam is the most common path by which you can be targeted for infection with a computer virus or social engineering. (Social engineering is when criminals psychologically manipulate people so that they divulge confidential information.)

2 Deter deceit

Avoid social engineering. Even if you have strong passwords, you can be tricked to provide information via social engineering. To avoid these scams, remember

- You will never be asked to provide credentials or personal data in an email or over the phone. Do not provide this information, even if the sender looks legitimate.

- Look for evidence that would suggest an email or website is fraudulent. Be suspicious if you see misspelled words, links to an unrelated website, or deals that are too good to be true.

Beware of ransomware. A type of malware, called ransomware, is designed to defraud unsuspecting users. It convinces you that your device is infected with a computer virus, and that you need to pay a fee to download software that will disinfect your computer. Rely on security software programs that are reputable, such as those available from TechSoup.

Browse the Internet more securely. Verify that a web page is legitimate before you enter any financial or personal information. For example, enter your bank's website address manually into your browser's address bar, rather than clicking a link to it in a questionable email, and make sure there aren't any typos.

In addition, look for websites whose addresses that start with "https." When you see this, it means that the website is using some form of encryption to protect the data that is transferred between you and that website. Most major websites employ HTTPS encryption.

Also, consider whether to have a computer or user profile that is dedicated to your organization's financial transactions (such as payroll or donor gifts). A dedicated computer or user profile would ideally have minimal Internet access and no access to email.

3 Establish policies for staff and volunteers

All staff and volunteers should read this guide. In addition, they should be informed of security risks that have been recently discovered. Also

- Establish a password policy for your organization and make sure staff keep passwords out of sight and secret.
- When new staff or volunteers come on board, train them so that everyone understands the risks and tactics to mitigate those risks.
- Establish an acceptable use policy for computers and mobile devices, and ask your staff members to confirm that they have read and understood it. Your policy should explain what users can do with the devices, what's allowed to be installed and stored, and what's allowed during non-business hours. The policy should also discuss replacement for lost or stolen devices.

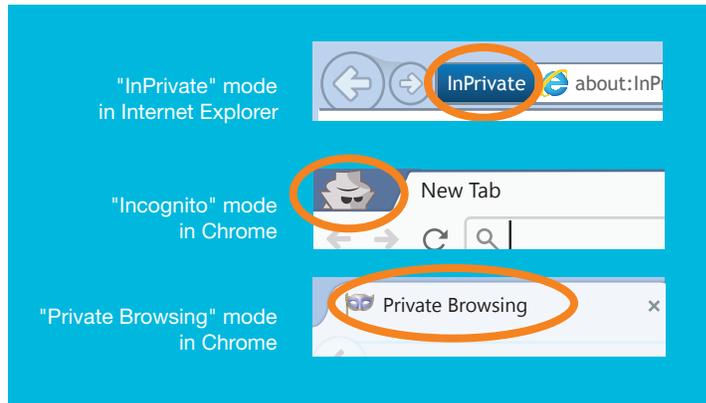


- Consider whether you can set up and support a discrete network like a subnet, or a "guest" wireless network with stringent controls. If this isn't feasible, we generally don't advise that staff members or guests use their own devices on your organization's network. If you do allow people to plug in to your network, implement a policy that's appropriate for your organization.
- Set minimum standards for the use of personal equipment or services for work purposes. For instance, you may want to require them to have antivirus software installed and to install security patches as soon as they're available. You should also advise employees to not use personal accounts for cloud storage, email, or any other service that takes sensitive data out of your organization's direct control.
- Use single sign-on wherever possible. It allows you to more easily manage account security across the organization by reducing the number of accounts for various services that you have to manage. It also makes it easier to revoke access to critical systems if you need to.

4 Secure mobile devices and remote workstations

Laptops, tablets, and phones are easily lost or stolen. Therefore,

- A mobile device should never be the only location for any set of important data.
- As with computers used in the office, restrict casual access to your device with a PIN or password.
- Any device that can be lost or misplaced should be encrypted. This precaution should include laptops.
- Be aware of malware, such as malicious apps that are designed to steal information. Think twice before you install any app, and only do so from reputable app stores.
- Use a cable lock to secure your laptop when left unattended, or stow it in a secure location like a locked cabinet or closet.
- Use GPS and location features on your phone or tablet only when you need to. It's true that this feature can be very convenient for personalization. However, location data that is included with your status posts or pictures could give hackers additional information that they could use for social engineering.



If your device is lost or stolen

- You might be able find it if you use its phone finder feature.
- If you can't find it, you might be able to remotely wipe all data from the device if it's online. Or, you may be able to remotely wipe all of the data the next time the device comes online.

5 Be vigilant when you use public computers

You should view every public computer as a security risk. This includes public computers at airports or stores, or computer labs that provide public access. These computers should already be in a "kiosk mode," in which data is not saved, but never assume that is the case.

If you must use a public computer

- Never use one for financial transactions.
- If you access email or social media, use the browser's "private" mode, which doesn't store any information after you close the browser. You can access this from the main toolbar where you'd normally open a new tab or window.
- Log out of all user accounts and close all open browser windows when you're done.

In a public space, you also need to be particularly aware of physical security.

- Don't leave the computer unattended with sensitive information on the screen.
- Be aware of individuals who could look over your shoulder. Avoid working on sensitive projects in a crowded area such as on a bus.
- Never insert your devices or drives into a public computer.



6 Be cautious when you use public Wi-Fi

You should treat all public Wi-Fi networks as insecure. This means you should

- Use public Wi-Fi networks only for nonessential Internet browsing.
- Never make financial or personal transactions over a public network.
- Consider safer alternatives. See if you could talk to a person via phone, or in person when he or she is available.

If you must connect to a public Wi-Fi network

- Connect to a network that has some security built in, rather than an "open" one. Such a network has a "lock" or "shield" symbol that's next to the network name. More secure networks require you to enter a password or agree to some terms or conditions before you can proceed.
- Beware of similarly named networks that are designed to fool users so that you log in. These networks may eavesdrop on your traffic. When in doubt, ask someone at that location to verify which network is the correct one.

Visit only websites that have an encrypted connection (look for website addresses that start with "https"). This prevents would-be eavesdroppers from being able to intercept your browsing.

A virtual private network (VPN) can help mitigate some of these risks when you use public networks. If you have staff who work remotely or travel frequently, consider whether you could set up a VPN.

If you have staff that frequently work from public locations, consider purchasing Wi-Fi hotspots that allow your employees to connect via a mobile broadband network and bypass public Wi-Fi entirely.

7 Social media is social (not "private")

Anything you post online is both permanent and transmittable. Everything you do on a social media site is also accessible by advertisers, and often may be more publicly accessible than you realize.

When you use social media, you should always

- Think carefully about how public you want your profile and information to be.

- Investigate and evaluate any site — especially its privacy settings — before you start to use it.
- Set appropriate boundaries on what you share online.
- Be selective about individuals you accept as "friends."
- Be vigilant when you meet someone in person whom you first met online, regardless of whether it's for personal or professional reasons. Do so in a public place and let others know of your whereabouts.

Social media is also a popular entry point for phishing and social engineering. (Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details [and sometimes, indirectly, money]. The phisher masquerades as a trustworthy entity or person in an electronic communication.) This is because users are by nature more likely to trust what their "friends" post. Exercise the same level of vigilance that you would with emails and websites.

8 Limit how much you share

Personal details can be used to defraud, impersonate, or find you. Things you post online could also affect your future job, credit, or insurance application and might reflect badly on your organization.

To ensure that you protect your privacy, safety, and reputation when you use social media

- Post only things that you would be comfortable to be heard in public.
- Don't post inappropriate pictures, videos, or comments.
- If you use a location service, consider whether you should limit who can access this information. Details about your location can easily be used for criminal ends. Criminals could spy on you, follow you, or steal something.

9 Be careful when your organization uses social media

Special care must be taken when staff and volunteers use social media on behalf of the organization. As with security, if new staff and volunteers will be active on social media channels, they should understand what is expected of them.

- Staff members should be cognizant that they should post or reply in a way that aligns with your organization's values. You should have a social media policy in place for your organization.



- If multiple users use a shared account, it's good to establish which staff does so when.
- If possible, use a social media publishing tool that allows staff members to publish to your accounts without requiring direct access to your social media account credentials.
- Some services offer different roles for different levels of privileges. Assign roles to staff as appropriate.
- If you "tag" or mention your constituents in a social media post, you might inadvertently reveal more information about them than you realize, so use this feature carefully.
- Unless permission is granted explicitly to use your constituents' imagery, blur their faces in your photos and videos.

10 Exercise caution with logins and consider whether to limit access to shared files

When your organization uses cloud services, anyone with credentials will be able to access the service. Each staff member or volunteer should have a unique login.

Many services employ two-factor authentication, where a login needs to be verified with a secondary device such as a mobile phone. Enable this feature whenever possible, especially for account-related changes such as passwords.

Users also must be careful about whom they grant access to online documents and files. Documents and files online are designed to be easily shared. Confirm the correct emails to use when you grant access, and consider whether the person needs both read and write access to the content.

11 Familiarize yourself with the cloud provider's policies

As a user of cloud services, you should be aware of the provider's policies in terms of data ownership and residency.

If authorities request your data, the service provider will likely comply and give your data to them. If your organization would protest a government subpoena of its data, then the cloud is not the right choice. Cloud data may also be more easily targeted by your adversaries.

A "private" or "hybrid" cloud, instead of the public cloud, may be more appropriate for you. Your decision about that option will depend on your organization's need for exclusivity.



This work is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported License.

You are free

 to Share—to copy, distribute, and transmit the work.

 to Remix—to adapt the work.

Under the following conditions

 Attribution—You must attribute the work to TechSoup (but not in any way that suggests that we endorse you or your use of the work).

 Share Alike—If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar, or a compatible license.

To view the full license, visit creativecommons.org/licenses/by-sa/3.0/ or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, CA 94041, USA.

12 Keep offline backups

Be prepared for the backup service to be unavailable. This applies for both free and paid options. Consider data that you want to put in the cloud, and how the inaccessibility of that information would affect your organization's ability to operate.

Download copies of your most important data so that you can access it even if the cloud service is unavailable. Your data should be able to be exported in a common format that you can use. If it isn't, consider whether you can change to a provider that does have that option.

There's often an audit trail of changes for online documents. Periodically review changes to see if there is unusual behavior.

The creation and translation of this guide was generously supported by Microsoft.