10 WAYS TO AVOID GIVING AWAY SENSITIVE INFORMATION

SEKUVA

1. Shop on safe, secure, and trusted websites

This means that you're using a connection that is secure (e.g. HTTP instead of HTTP) and that you're on a safe website belonging to a credible company.

Not sure if you're on a safe website? Scan the website in VirusTotal. VirusTotal is a free virus, malware, and URL online scanning service.

2. Use your credit card instead of debit card when paying

Credit cards provide more safety since they offer better protection and can easily bounce back from a fraud or fraud attempt.

You can also use a service like PayPal, Apple Pay, or another mobile payment application which offers even more security than using a credit card.

3. Browse through a safe connection

Make sure that you're using a safe internet connection so that you're protecting your valuable information online. When you use a non-safe connection, everything you do online is visible. This includes your login information and credit card details.

Practice using safe home wi-fi, VPN, or cellular data.This is the best way to connect online. If you use public wi-fi, install a VPN. A VPN creates a secure connection even when using public wi-fi. You want to make sure that your sensitive financial and personal information are in the right hands.

4. Share less

Sharing often seems harmless, but the ramifications of sharing too much are huge. Other than privacy, most people don't realize certain information that they share can be used to guess security questions. Like the name of your dog, childhood best friend, favorite teacher, and street you grew up on.

5. Check your statements regularly or enable bank account notifications.

Make sure you're up to date with all of the activity going on in your account. It's better to catch something sooner rather than later!

6. Create secure and complex passwords

Passwords are the key to all of your account information. This is why there is so much emphasis on making it complex. It's important to note that complex means focusing on length instead of random numbers and symbols. Think of your password as a "passphrase" and come up with something nice and long. Also, inserting spaces adds more security to your passphrase.

Examples:

Thecatseemsgreathere_45~!
versify ardor holdover till becalm acoustic
delphi-cult-dignify-brisket-pummel-news

Remember that passwords are only as secure as how you manage them. In other words, make sure you're not storing your passwords in your email, online notes, excel sheets, google docs, word applications, or sticky notes on your desk.

It may seem that I ruled out all options of storing passwords but there are two ways to securely store passwords:

1. A password manager
2. A notebook stored in a safe and secure place

7. Keep all software and hardware updated

Make sure that your applications and computers are up to date. Even your browser needs to be updated.

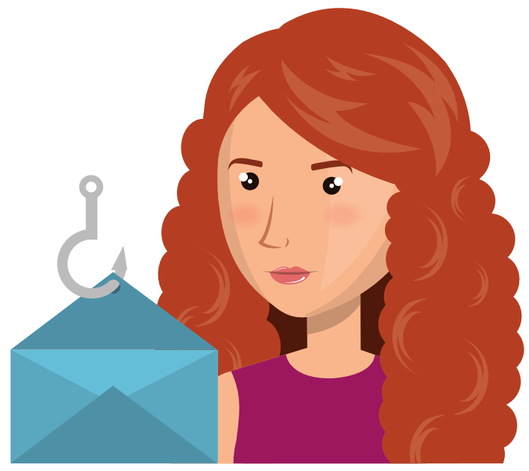
Consider enabling automatic updates so you don't miss one. Updates are important because they patch weak points in systems in order to safeguard against the risk of sensitive information getting into the wrong hands.

8. Backup all of your important data

Backing up your data is one of the most important things you can do. It usually doesn't seem so until something unfortunate happens and you lose your precious photos or sensitive information that you didn't store anywhere else.

The best step to take is to determine how often you will back up and to where. There are many inexpensive options and you can also set up automatic backups in some cases.

9. Be cautious of emails that claim to be a legitimate busines

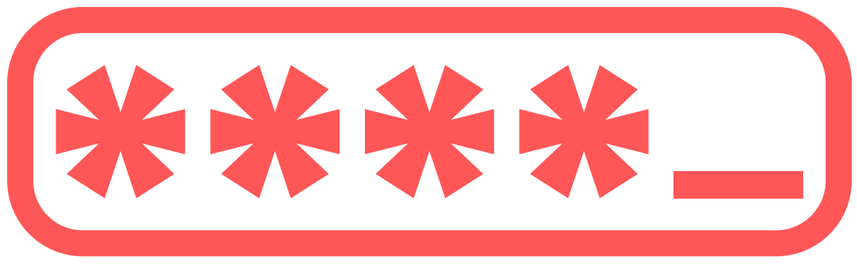


Many scam emails will pose as popular businesses like Amazon, Netflix, or Microsoft. They'll say anything to get you to click on a link or download something. If you get an email like this, make it a habit to always visit the known website and not the website provided in the email.

This allows you to see if what they claim in the email is in fact true. Developing this habit will lessen the likelihood of mistaking a criminal for a legitimate business.

10. Enable two factor authention on all accounts

Two factor authentication provides another means of authenticating to an account. This security feature prevents hackers from trying to access your account by having you supply a code, fingerprint, or hardware device to prove you're who you claim to be.



Was this valuable?

Join the "Online Security Movement" FB group for more tips, tricks, discussions, and new scam alerts!