The bridge to possible

10 Cybersecurity Tips for the Solopreneur

As a solopreneur, you're doing it all: sales, marketing, accounting and even being your own risk manager. That's why it's so important to manage risk by prioritizing the protection of your assets.

Safeguard your business with these 10 tips:

1 Use Strong and Unique Passwords for Each of Your Accounts

As cybersecurity threats increase, this is the easiest way to secure your devices, accounts, and sensitive information. Never use the same or similar passwords for all your accounts and applications.

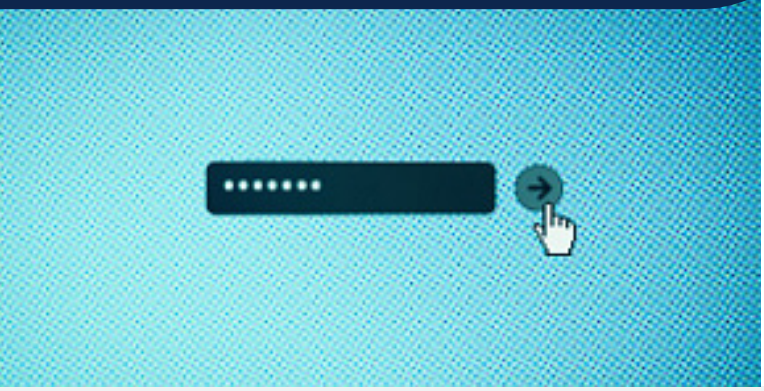
Strong and unique passwords should include at least:

- one capital letter
- one lowercase letter
- one number
- one special character
- 8–12 characters (the longer, the better)

Avoid using accessible personal information in your passwords. For example, never use your street name, your pet's name, or number sequences like "1234". Don't save your passwords within browsers or applications, since they're threatened if your accounts are hacked.

Use a Password Management Tool

2



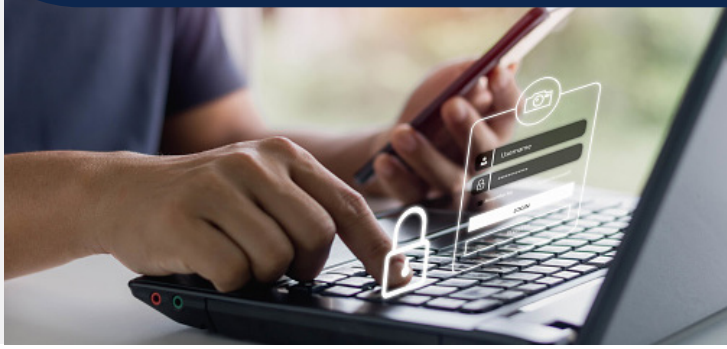
This trusted application manages and stores your passwords for you, so you don't have to memorize numerous complex passwords, which can be challenging.

Your passwords are protected by one strong and unique master password. Master passwords should be changed often.

Use Multi-Factor Authentication (MFA)

3

This access security product verifies a user's identity by adding identity-checking steps at login. If your financial institution doesn't offer MFA, switch to one that does, or try Duo MFA for free.



Establish a Virtual Private Network (VPN)

4

Establishing a VPN places a private network onto a public network enabling the user to send and receive data to their device that otherwise would only be allowed if the device is connected to a private network.

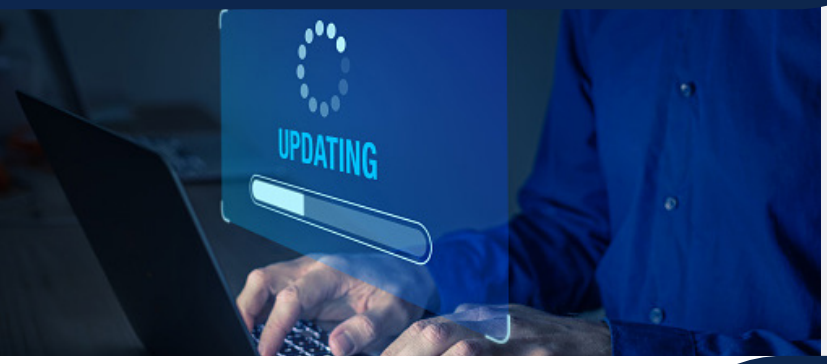
To set up a VPN, select a VPN application, set up an account, and define the location the VPN will be connecting to. It is wise to select a location close to your physical location – proximity of the server leads to a faster connection.

5 Perform Regular Data Backups for Both Business and Personal Data

If your device crashes or becomes corrupted, a backup will help you recover your data.

Set up automatic backups on each of your devices. If your device does not have automatic backups set a daily or weekly reminder to complete them.

6 Update Software When Prompted



Having outdated software subjects your device, personal information, and finances to vulnerabilities. Software updates also benefit device functionality, as outdated software can hinder optimal performance.

7 Add a Compatible Antivirus Program to Each of Your Devices

Dangerous malware threats come in viruses, spyware, worms, and other forms, and these continue to evolve in sophistication.

Proactively protect your devices by installing antivirus programs to safeguard your data and your company.

Beware of Phishing and Smishing

8

With these attacks, bad actors send you corrupted links in email (phishing) or text messages (smishing) that appear to be from trusted senders. Since you're a busy solopreneur, attackers count on you to make the simple mistake of clicking on a malicious link, enabling them to gain access to your information.

Stop and think before you click, and look for these red flags:

- Verify the sender, and carefully review their email to make sure it's a trusted party
- Identify any discrepancies, like typos in the subject and body of the email
- Hover over links, to preview the destination URLs, and verify their credibility
- Beware of urgent requests or those collecting personal information

If you're unsure, contact the company using their official channels to confirm the validity of the message.

9 Protect Your Personal Information

Do not store personal information such as business financial data and account numbers or tax information on unprotected devices or online.

For physical files containing personal data, do not store them in easily accessible places. Consider locking up your sensitive files in a cabinet that only you can access.

Manage Your Business Data and Personal Data Separately

10

If you use a single system and you are compromised, your attacker has access to both your work and personal assets. Have two unique computers; one for business, the other for personal use.

If you must use a single device, we recommend managing separate password-protected accounts for your business and personal applications, such as email, banking, and credit cards.

Secure tomorrow, together

Share your knowledge to help others become more cyber aware.

For more information,
visit trust.cisco.com