2020 PASSWORD PROTECTION GUIDE

CRASHPLAN
For Small Business

CRASHPLAN

PROTECT YOUR PASSWORDS

Password hygiene best practices.

Passwords are everywhere, and are used to protect your most sensitive data, whether that is financial data, health data, or just your favorite family vacation photos. Because passwords are so important, criminals are always working to capture, compromise, or otherwise gain access to passwords to get to things that they shouldn’t.

THERE ARE SEVERAL WAYS THAT PASSWORDS CAN BE COMPROMISED:

Brute Force Attack: A brute force attack is when an attacker tries a very large list of possible passwords, such as words from a dictionary, to try and guess the right one.

Credential Stuffing: Credential stuffing is when an attacker takes a large list of usernames and passwords from a data breach and tries them against other services, like banking websites, to determine if those passwords were reused and thus provide access to the account.

Hash Cracking: Hash cracking is when attackers gain access to a database of stored passwords that have been hashed, which is a way of obfuscating the password. They then attempt to reverse the obfuscation to get the original password.

With so many ways to compromise passwords, it may seem like it is impossible to protect your password and keep it safe. That is definitely not the case! By consistently engaging in a few password and account best practices, you can dramatically reduce the chance that your accounts will be compromised:

- **Use strong passwords:** Use long passwords or passphrases that are complex and combine uppercase letters, lowercase letters, numbers, and symbols. The best passwords are long (more than 16 characters) and completely random.

- **Never reuse passwords:** Use a separate password for each service you use.Be careful where you enter your password: Beware of entering passwords on websites that don't show the lock indicating that traffic is encrypted, links that you get via email, and untrusted wireless networks.

- **Enable Two-Factor Authentication:** While not strictly a password best-practice, enabling two-factor authentication (2FA) on every service that has it means that even if your password is compromised, the second authentication factor, such as an SMS text or a time-based code from an app like Google Authenticator, is still protecting your accounts. You can enable two-factor authentication for your Crashplan for Small Business by following the instructions here.

Of course, it's next to impossible to keep all of those long, random passwords in your head, so using a **password manager** makes generating, saving, and using passwords much easier. There are many free password managers available that can manage your passwords for you, as well as paid services that provide cross-device syncing, sharing, and reporting. Choose whatever tool works best for you, as a password manager does no good if you don't use it!

By taking these steps to protect your passwords, you can rest easy knowing you are doing all you can to protect your private data.

CRASHPLAN
For Small Business

2020 - PASSWORD PROTECTION