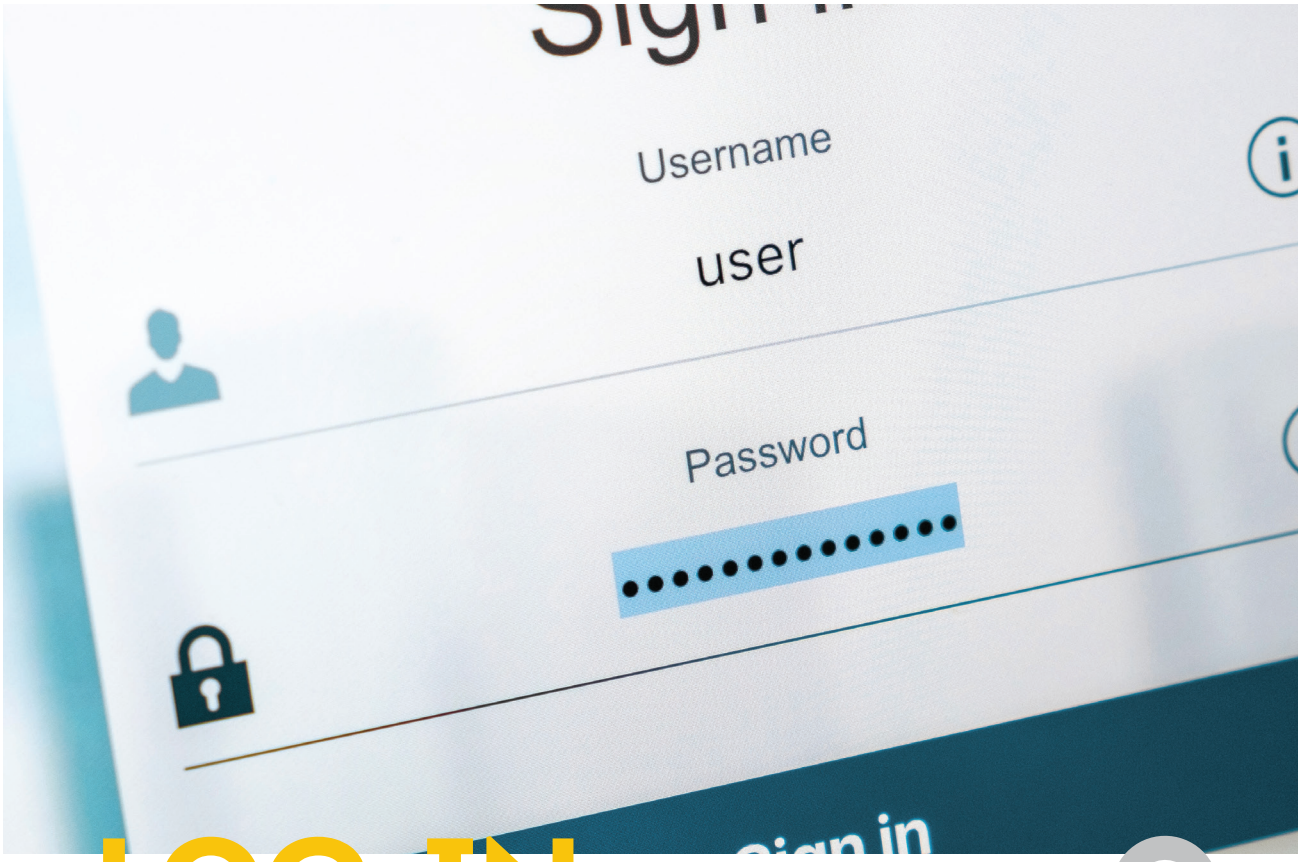
Synchrony Connect

synchrony
CHANGING WHAT'S POSSIBLE™

LOCK DOWN YOUR

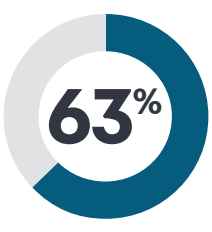


LOG-IN

Every organization today – no matter its size – is in the business of data. You wouldn't leave the doors to your office or store unlocked overnight, right? Well, failing to enforce a strict company password management policy is like leaving your business premises unlocked at the end of the day. As your company grows, so will your users, accounts, and data; so, it is best to implement good password management as soon as possible!

Employees are an easy target to hackers because more than 80% of data breaches start with an employee as a victim and, 63% of confirmed data breaches involved leveraging weak, default, or stolen passwords.

of data breaches start with an employee as a victim



of data breaches involved leveraging weak, default, or stolen passwords

Synchrony Connect

synchrony
CHANGING WHAT'S POSSIBLE™

FIRST STEP: AUTOMATION

Take password management seriously and start with automation. Below are some policies and tools to help require strong passwords and good password hygiene.

Click here for the full password recommendation from the National Institute of Standards and Technology (NIST).

Password Length. Configure your systems to have a minimum password length of at least 8 characters (12 or 14+ characters are even better). Support longer passwords, 64 characters is recommended).

No complexity requirements. If you do use complexity requirements, do not disclose when logging in.

Don't restrict characters. Support all characters, including the space. Use password awareness training and content guidelines to encourage complicated password with a mix of characters (numbers, capital letters, and special characters).

Restrict sequential or repetitive characters
(i.e. 12345 or aaaaa)

Restrict context specific passwords
(i.e. name of company, year)

Restrict commonly used passwords
(i.e. p@assw0rd, Click here for the most common passwords of 2019)

No password hints.

Security is unique to the company, so implement what is manageable and secure enough for your company, employees, and customers. **Some security is always safer than none.**

DOUBLE DOWN WITH TWO-FACTOR AUTHENTICATION (2FA)

Passwords are the key to most accounts and anything you do online. Unfortunately, even the strongest passwords can be hacked, stolen, and unintentionally shared. **2FA is here to lock down your login.**

2FA adds an additional level of security when logging in so someone can't gain access with only your username and password. 2FA requires a combination of something you have (device, security coin, ID card), something you are (fingerprint, face, voice), and something you know (password, PIN, authentication questions). NIST encourages the use of 2FA types other than SMS or knowledge-based authentication, such as one-time password from applications. Click here for more information on 2FA.

Most accounts and systems offer 2FA; so, **enable 2FA whenever possible and require it for your employees.** 2FA is an additional protection not a substitute, so do not forget about strong password management and good password hygiene.

CLIENTS AND CUSTOMERS

Use password requirements to automatically help customers prevent hackers from accessing their accounts. Make sure you find a balance of convenience and security. Some industry norms are as follows: password length and complexity requirements, authentication questions, two-factor authentication.

SECOND STEP: AWARENESS

Automation only goes so far in securing your business. Finish the job by talking to your employees and clients about good password hygiene and offering tools to make password management easier.

Routinely review password hygiene practices with your employees. Topics to cover: Don't share or write down your password, company password policy (length, complexity, etc.), importance of passwords, etc.

Teach employees to easily create strong and memorable passwords. Click here for a video by Habitu8 on a quick and easy way to create a strong and memorable password.

Offer a Commercial Password Manager. Password managers are the answer to password reuse and people writing down their password. There are many free or low-cost options so pick one and use it as your organization's password manager of choice.

PASSWORDS ARE THE KEY TO EVERYTHING. KEEP THEM STRONG, LONG, AND COMPLEX.

For more information or to connect with an expert, contact us at synchronyconnect@synchrony.com.