2-Factor Authentication

2-Factor Authentication is an extra layer of security that is used to verify that the person logging into an account is who they say they are. Normally when you log in to one of your accounts you use just your username and password. When using 2-Factor Authentication a user will enter their username and a password. Then they will have to enter another piece of information. This second piece of information is broken into 3 categories.

- **Something you know:** This could be a personal identification number (PIN), answers to “secret questions” that you set up beforehand, or a specific keystroke pattern. The most common form would be security questions, such as your first pet or your best friend’s name.
- **Something you have:** Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token. The most common form would be getting a code texted to you.
- **Something you are:** This category is a little more advanced, and might include a fingerprint, a face scan, or a voiceprint. You can find these on your phones when you use your fingerprint or face scan to open your phone.

2-Factor Authentication makes sure that your account is secure even if you lose your phone or your passwords are compromised. The chances that someone else would have both your password as well as your secondary information is highly unlikely.

Common Types of 2-Factor Authentication

SMS Text-Message and Voice-based 2FA:

This type of 2-Factor Authentication directly interacts with your phone. After you enter your username and password, the site sends the user a unique one-time passcode through a text message. The user then needs to enter that code into the site to gain access. Voice-based 2-Factor Authentication is similar. The site will automatically dial the user and a robot will read out the code for the user to enter. However, this is considered the least secure form of authentication as hackers could intercept the code as it was being sent.

Software Tokens for 2FA:

This is one of the most popular forms of 2-Factor Authentication. With this form of authentication, the user downloads an app to their phone or computer that generates a new code every minute. The website will prompt the user to enter that code when they try to log in. The user will then look at the app and enter the code shown there. In this form of authentication, the website might have its own app that generates the code or use a third-party app such as Google Authenticator or Authy. With the app, the code is generated on the phone itself so there is no chance of hacker interception.

Push Notification for 2FA:

With this form of authentication websites and apps can send the user a push notification on their phone alerting them that someone is trying to log in. The device owner can then approve or deny access by tapping the screen.

Biometric 2FA:

This form of authentication isn't very popular with the average person yet. Is currently being used mainly as the primary form of authentication for cell phones and some computers. However, it is popular in the professional environment.

According to a recent report, stolen, reused, and weak passwords remain a leading cause of security breaches. Unfortunately, passwords are still the main (or only) way many companies protect their users. There are still some companies and websites that don't support 2-factor authentication. When creating an account online you should ask yourself what you are giving to the site. If you need to put in a lot of personal information such as on Facebook or Instagram it would be a good idea to enable 2-factor authentication. You can check what sites support 2-factor authentication at https://twofactorauth.org/. There you will be able to see if a site where you are creating an account has 2-factor authentication enabled before you make the account.