Cybersecurity: Protecting You and Your Loved Ones On-Line

Multi-Factor Authentication is a security protocol method in which a computer user is granted access only after successfully presenting two or more types of validation credentials. For example, a password and a code sent to your phone or email.

Most web sites that house sensitive personal information and require usernames and passwords offer an ability to implement MFA, although it is often referred to by different names. The process required to set up MFA is unique to individual web sites and may vary depending on how a web site is accessed, but typically involves following steps outlined within "Settings" and "Security". Directions specific to some of the more popular online destinations follow below.

Multi-Factor Authentication Implementation Instructions

Amazon

Sign in to your Amazon account, click "Account & Lists" at the top right and then go to "Your Account" > "Login & Security Settings" and click the "Edit" button for "Advanced Security Settings". Click the yellow "Get Started" button and sign up to receive codes via SMS or an authenticator app. You will also need to add a backup phone number to reduce the odds of getting locked out of your account.

Apple

From an iOS device, go to "Settings" > "Passwords and Accounts", "iCloud", sign in and then tap on your Apple ID. From your Apple ID page, tap "Password & Security" and then tap "Turn On Two-Factor Authentication". On a Mac, you can enable it by going to "System Preferences" > "iCloud" > "Account Details" > "Security" and clicking "Turn On Two-Factor Authentication."

Facebook

Click the triangle button at top right, go to "Settings" > "Security" and then click "2 Factor Authentication" and "Select Security Method".

Google

Head to Google's 2-Step Verification page, click the blue "Get Started" button and sign in to your account. You can choose to receive codes via text or a voice call. You can also set up and print backup codes, add a backup phone number, and set up Google's Authenticator app. You can also sign up to use Google prompt, which sends a notification to your phone that you can simply tap instead of having to enter a code.

LinkedIn

Go to the "Security and Passwords", then "Account" and click "Add a Phone Number" if you haven't already done so. With your phone number added, click "Turn On" next to where it says "Two-Step Verification is Turned Off", enter your account password, and then enter the verification code that LinkedIn sends to your phone.

Microsoft

Go to the "Security Settings" page, sign into your Microsoft account and click "Set Up Two-Step Verification". You can choose to receive codes via email, text or via the Microsoft Authenticator app. You'll also need to create an app password to continue to use Microsoft devices and services that don't support MFA, such as the Xbox 360 and Outlook.com email on an iPhone or Android phone.

PayPal

Log in to your account and click the gear icon in the top right to enter "Settings". Click the "Security" tab and then "2 Step Authentication". Enter your mobile phone number and then the verification code that PayPal sends you.

Yahoo

In your Yahoo Account, go to "Account Security" and toggle on "Two-Step Verification". If you have Yahoo's Account Key enabled, you'll need to disable it. Account Key looks and smells like two-factor authentication but it is really only one-factor; it lets you skip the first factor of entering your password and only enter a code sent to your phone. Yahoo's two-step verification is the more secure option of the two. You can also create app-specific passwords for any apps that don't support MFA and use your Yahoo account.

How can we help you? Please contact:
Jim O'Neil, Managing Director, 617-338-0700 x775
privateclient@appletonpartners.com
www.appletonpartners.com