Security Best Practices - Part 1a: Two-Factor Authentication

Travis - 2021-03-16 - Best Security Practices

1a. Two-Factor Authentication

In addition to having a password with high password entropy (password strength), it's still not effective if your password were to fall into the wrong hands. In our day and age of ever-growing cybersecurity threats, the once-mighty password has become an outdated security measure if left to operate alone. The implementation of two-factor authentication is almost an essential step in the modern era of online security. Two-factor authentication is a system that double-checks the attempted login is actually coming from the owner of the account and will deny entry unless approval is granted by the second factor. There are several forms of 2FA commonly used today.

2FA Options

Acceptable

Verification requests can be sent via SMS text message, email, or even through a phone call to have a user prove their identity. Some inherent flaws with these methods are they require the user to have a cellular or landline phone connection to receive the texts or voice calls or an internet connection to receive the email verification. Those messages are also

normally not encrypted and email accounts are easily broken into.

Optimal

Hardware tokens can also be used in the form of a USB device that sends the verification once engaged. These can be a more secure and reliable form of 2FA compared to the former. They require a separate device to grant permission and can be programmed to transfer the 2FA code based on the length the device is engaged, such as a finger press. While this alternative form of 2FA is more secure, they can be expensive and rendered useless if lost as they tend to be on the smaller side.

Superior

Two-factor authentication paired with a smartphone (push notifications or codes), which according to Bankmycell 48.46% of the world population uses, the threat of account access due to a compromised password is almost completely nullified. Having 2FA tied to a smartphone authentication application becomes more secure as the app generates time-based, one-time passcodes that rotate at short intervals, depending on the app. With 2FA linked to an authentication app, it removes the need to have the account linked to a phone number and rather just the device, which can be easily reinstated if the device or number changes. Even if your smartphone is lost or the battery is dead, PIA provides 10 recovery codes that can be used to access the account, as long as they are securely stored upon our 2FA setup.

We would encourage all of our users, if possible, to set up 2FA for their PIA accounts to add that additional layer of security. Beyond just PIA, 2FA should be taken advantage of for any service that offers it, providing some additional peace of mind when it comes to protecting your online well being. For additional information on setting up 2FA for your PIA account, please review our article on the setup process here.

Tags

Security

Related Content

- How do I enable and use Two-Factor Authentication?