OUCH! September 2021

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for You

One Simple Step to Securing Your Accounts

Does it seem like cyber criminals have a magic wand for getting into your email or bank accounts and there's nothing you can do to stop them? Wouldn't it be great if there was one single step you could take that would help protect your from cyber criminals and let you securely make the most of technology? While no sole step will stop all cyber criminals, one of the most important steps you can take is to enable something called two-factor authentication (sometimes called 2FA, two-step verification, or multi-factor authentication) on your most important accounts.

The problem with passwords

When it comes to protecting your accounts, you are most likely already using some type of password. There are several ways to authenticate yourself into an account: something you have, something you know, something you are, somewhere you are. When you employ more than one method of authentication, you are adding an additional layer of protection from cyber criminals – even if they crack one method, they'd still need to bypass the additional factor(s) to access your account. Passwords prove who you are based on something you know. The danger with passwords is that they are a single point of failure. If a cybercriminal can guess or compromise your password, they can gain access to your most important accounts. In addition, cyber criminals are developing faster and better techniques at guessing, compromising, or bypassing passwords. Fortunately, you can fight back with two-factor authentication.

Two-factor authentication

Adding two-factor authentication is a far more secure solution than relying on just passwords alone. It works by requiring not one but two different methods to authenticate yourself. This way if your password is compromised, your account is still protected. One example is your ATM card; when you withdraw money from an ATM machine, you are actually using a form of two-factor authentication. To access your money, you'll need two things: your ATM card (something you have) and your PIN number (something you know). If you lose your ATM card, anyone who finds your card cannot withdraw your money as they do not know your PIN. The same is true if they only have your PIN and not the card. An attacker must have both to compromise your ATM account. The concept is similar for two-factor authentication; you have two layers of security.

Using Two-factor authentication online

Two-factor authentication is something you set up individually for each of your accounts. It is actually quite simple: you usually need to do nothing more than syncing your mobile phone with your account. That way when you need to log into your account, not only do you log in with your account username and password, but you also use a unique one-time code you get from your phone. The idea is the combination of both your password and unique code are required to log in. Usually, this unique code will be sent via a text message to your mobile device or email. Your phone may also have a mobile app (such as Google or Microsoft Authenticator app) that will generate the unique code for you. When possible, mobile apps are considered the most secure option for obtaining your unique code.

What makes this so simple is that you usually only have to do this once from whatever computer or device you are using to log in. Once the website or your account recognizes your device, moving forward you often only need your password to login. Any time you try (or someone else tries) to log in with your account but from a different computer or device, they will have to use two-factor authentication again. This means if a cybercriminal gains your password, they still can't access your account as they can't access the unique code.

Remember, two-factor authentication is usually not enabled by default, so you'll have to enable it yourself for each of your most important accounts, such as banking, investments, retirement, or personal email. While this may seem like more work at first, once it's set up it's very easy to use.

Guest Editor

Lysandra Capella has over 15 years of experience working in Information Security and Technology. She is a SANS Institute Instructor in Training for SANS AUD507, focused on measuring and managing risk. When not teaching, Lysandra supports executive management teams with strategy formulation, security assurance and IT governance. https://www.linkedin.com/in/lysandracapella/.

Resources

Keeping Passwords Simple: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Password Managers: https://www.sans.org/newsletters/ouch/password-managers/