Workforce Security and Risk Training

The Monthly Security Awareness Newsletter for You

How to Ruin an Attacker's Day? With MFA!

Easy for You is Easy for an Attacker Too

James was relaxing at home when his phone suddenly erupted with notifications. The password for his personal email account had been changed, but he didn't remember changing anything. Soon after, his social media accounts followed, alerting him that those passwords had been changed, then his bank alerted him to suspicious purchases. Panicking, James tried logging into his email, but his password no longer worked. Someone had locked him out! Over the next several days, James spent hours recovering accounts, disputing charges, and changing passwords. What confused him most was that he had done everything he thought he was supposed to do. He used a strong password and never shared it with anyone!

But his password wasn't the problem: the problem was relying on just the password alone. What James didn't realize was that the urgent text message he received last week from what he thought was his email provider was actually from a cybercriminal, who had tricked him out of his password. Once the cybercriminal obtained the password to James's personal email, they had complete control of his email account. Not only were they able to access all of James's emails, but they could use his email account to reset the password on many of his other accounts.

James's sister, Ariel, received the very same text message, and just like her brother, she was tricked into clicking on the malicious link and entering her password. However, unlike James, Ariel used Multi-Factor Authentication (MFA) to protect her email account. This meant that the attacker was missing a second factor needed to log in, separate from the password, and had a frustrating day of unsuccessful logins. Ariel blocked the attacker, secured her email, and had a much better day than James. Soon after, she helped her brother set up MFA so he could ruin an attacker's day, too.

What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication, or MFA, is a free and simple way to add an extra layer of security to your accounts. Instead of relying just on your password, MFA adds a second step (or factor) to prove it's really you. With MFA, logging in typically requires at least two of the following:

- **Something you know**: your password
- **Something you have**: a one-time code sent to your phone or generated by an app
- **Something you are**: a fingerprint or facial recognition

Even if a cybercriminal steals your password, they still cannot access your account without that second factor. This is why enabling MFA is often considered **the single most important step you can take to secure your accounts**.

How to Use MFA the Right Way

The good news is that MFA is simple to use and widely available. Most major services (email, banking, social media, and shopping sites) offer it for free. Even better, often you only have to log in once with MFA for each site. After that, the website learns and remembers your browser, making authentication not only stronger but simpler. Here's how to get started:

1. Turn on MFA for your important accounts: Start with your most critical accounts: email, banking, investments, and any other important accounts. Remember, if someone gets into your email, they can often reset access to your other accounts.

2. Use an authenticator app when possible: One of the most common ways to receive your second factor is having a unique code texted to your phone. However, using a dedicated authenticator app is an even more secure and reliable method. An authenticator app is a mobile app you install on your phone that generates one-time codes for you to use, rather than having them texted to you.

3. Combine MFA with strong passwords: MFA is powerful, but it works best alongside strong, unique passwords. Always use a strong, unique password for each of your accounts in addition to MFA. If you are seeing websites asking you if you would like to enable Passkeys for your account, a Passkey is just a very secure version of MFA.

4. Protect your mobile devices: Your mobile device has now become essential to implementing MFA, and may also contain your password manager, in many ways holding all of the keys to your kingdom. Keep your mobile device secure by enabling a screen lock and automatic updating.

Take Control of Your Security

Enabling MFA is one of the most powerful ways to protect yourself online. Don't wait until after your accounts are compromised like James's. Be like Ariel, and make sure it's the attacker who has a bad day.

Guest Editor

Betta Lyon Delsordo, a Penetration Tester at AWS, specializes in application, cloud, and AI security. She holds a Master of Science in Cybersecurity from Georgia Tech, and the GPEN certification. Betta's speaking history includes DEF CON, the World Bank, WiCyS, and conferences across the US and EU.

Resources

How Cybercriminals Steal Your Passwords: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions
The Power of the Passphrase: https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter
The Power of Password Manager: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch