Cybersecurity Awareness Month 2022: Enabling Multi-factor Authentication Key behavior: Multi-factor Authentication

October 4, 2022

By: Bill Newhouse and Ryan Galluzzo

https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-2022-enabling-multi-factor-authentication

In celebration of Cybersecurity Awareness Month, NIST will be publishing a dedicated blog series throughout October; we will be sharing blogs each week that will match up to four key behaviors identified by the National Cybersecurity Alliance (NCA). Today's interview-style blog features two NIST experts —Bill Newhouse and Ryan Galluzzo— discussing different reasons to enable multi-factor authentication (a mechanism to verify an individual's identity by requiring them to provide more information than just a username and password).

Here are [some of] the questions they both were asked, along with their responses:

What is the easiest way to stay safe online?

Bill: Be intentional—Unless you turn off your computers, tablets, fitness trackers, and mobile phones, you are online. So, if you are always online, increase your online safety by using devices and applications that are supported by automatic security updates. From this foundation, staying safe online also means being as intentional as possible. One way I am intentional is that I enable multi-factor authentication (sometimes called 2-step verification) for all online accounts that hold sensitive or precious-to-me data. If I don't want to lose control of my account, I visit the security section of my customer profile and turn on MFA which allows me to leverage "authentication apps" that provide randomly generated one-time codes or push notifications, a hardware authentication device that supports public-key cryptography, or I use my mobile device's built-in biometrics.

If I seek to enable MFA to support online access and the provider does not offer it, I will not continue to be a customer.

Being intentional also means that I try to control the sites I visit. I likely spend more time than most looking at the web addresses when on my browser as I surf the web. If I get

an email indicating something about an online account that offers me a link to take an action on that account, I don't immediately click the link. I don't want to become a victim of a phishing attack, so I tend to access my online account's customer portal without having clicked on a link. I like being in control by taking that extra step to open a new browser tab and type in the URL for my customer or user access to that online service.

Ryan: Adding multi-factor authentication to all your sensitive accounts. Many service providers have made this easier than consumers may realize. Proliferation of smart mobile devices have given individuals many more options than had previously been available. From "authentication apps" that provide randomly generated one-time codes or push notifications, to native biometrics on our devices, there are more options for securing our digital selves than ever. The increasing ubiquity of federation has also helped, allowing users to sign in with common providers, where MFA is sometimes incorporated by default. Many of us are probably using MFA every day – particularly with our mobile devices – and simply don't even realize it.

You may not need MFA for everything – but if your personal information, financial information, or health care data is involved you should make sure to check your providers account settings to see if you can turn it on. I would also consider moving away from using text-based MFA for these services in favor of an authenticator app. These typically offer several different methods to authenticate with different websites and can typically be set up quickly and easily by scanning a QR code. If you are feeling particularly paranoid – or nerdy – hardware tokens and authenticators that use cryptographic authentication (like FIDO tokens) can further increase your digital security by improving resistance to phishing attempts.

What are three things you can do to minimize cybersecurity risks to a person or businesses?

Bill:

- Turn on MFA on for all of user accounts. Make it mandatory to use MFA for employee access to the business' devices, networks, and services on which your employees conduct their work.
- Employees who need remote access to your business' network and security resources should use a virtual private network (VPN) connection. If an employee is not directly connected to your network, they are relying on networks that your business does not control. Using VPN technology for remote access shields your business' data and process from prying eyes.
- Train your employees to use MFA. The more you learn about the risks you face when you don't enable MFA for any access to an online system or service, the more likely your employees will embrace the use of MFA.

Ryan:

- Turn MFA on for all your sensitive accounts. Check your account settings or security settings to see if it is an option. It is probably more available and easier to use than you

think. If you are a business, consider default MFA for all your enterprise users. Avoid weaker forms of MFA that are more easily compromised or phished such as text-based OTP. For users with elevated privileges, consider cryptographic authenticators such as hardware tokens or FIDO authenticators.

- Use a VPN when connecting to any unsecure or public networks. This is particularly true when you are conducting sensitive transactions – such as banking – but is a good default security setting, regardless. Businesses should mandate the use of VPN access for all company assets and consider mobile device management solutions to enforce security baselines for company or personal phones used to conduct business.
- Educate yourself…and if you are a business, educate your employees. Humans are always the weakest link in the security chain. The more you learn about the risks you face, the more likely you are to identify when you are being deceived or targeted. For organizations - have an established, interactive security education program that teaches your employees what to look for in common attacks – such as phishing, social engineering, and business email compromise.

What does #BeCyberSmart mean to you?

Bill: From a very practical point of view, #BeCyberSmart means I can search Twitter to find posts that touch on different aspects of staying safe online using the hashtag #BeCyberSmart. Good advice should not be hard to find. DHS created the #BeCyberSmart campaign to help you find good advice for staying safe online.

Ryan: Vigilance. Just like safety in the real world, security in the digital world revolves around being aware of the threats you face and keeping an eye out for those things that "just don't look right." Even if you are using MFA there are still risks – particularly when using text and one-time codes. Just as you would never input your password on a website that looked sketchy, don't provide MFA codes to sites you don't trust or may not look legitimate.

ABOUT THE AUTHORS

Bill Newhouse

Bill Newhouse is a cybersecurity Engineer at the National Cybersecurity Center of Excellence (NCCoE) in the Applied Cybersecurity Division in the Information Technology Laboratory at the National Institute of Standards and Technology (NIST).

Ryan Galluzzo

Ryan is the Digital Identity Program Lead for the Applied Cybersecurity Division at the National Institute of Standards and Technology (NIST). In this role he coordinates digital identity projects, initiatives, and efforts to advance NIST's standards & guidance and drive foundational research to promote innovation in digital identity. He has contributed to multiple NIST Special Publications including NIST SP 800-63 *Digital Identity Guidelines*. Prior to joining NIST, Ryan was a Specialist Leader at Deloitte & Touche where he spent over 10 years providing cybersecurity and identity management subject-matter insights to multiple federal agencies, including the Internal Revenue Service (IRS), the General Services Administration (GSA), and NIST.