Week 1: Cybersecurity Awareness Month - Multi-Factor Authentication (MFA)

By now, we should all be familiar with the prompts to verify our identity with a text or phone call from Microsoft. Every 90 days, or when you connect at a new location, you will be asked to verify your identity. Multi-factor authentication (MFA) prevents criminals from accessing your account even if they have obtained your password. This extra layer of protection has had a tremendous impact on keeping our network safe.

Reminder: When logging into your email or any other Microsoft applications (Outlook, Word, Excel, etc.) you may be prompted to "Verify your identity." Choose either a phone call or a text message to your phone. (The last two digits of your number display):

a. If you select call option, Microsoft will call your phone in seconds. The recording asks you to press the pound key "#" on your **phone's keypad**.

b. If you select text message, Microsoft will text your phone in seconds. Check your phone for a text message with a code to enter on your computer screen.

When successful, either option offers you access to your email or application.

Note: There is now a 3rd option for verifying your identity. If you choose, you can use the Microsoft Authenticator App to verify your identity. This app can be downloaded from:

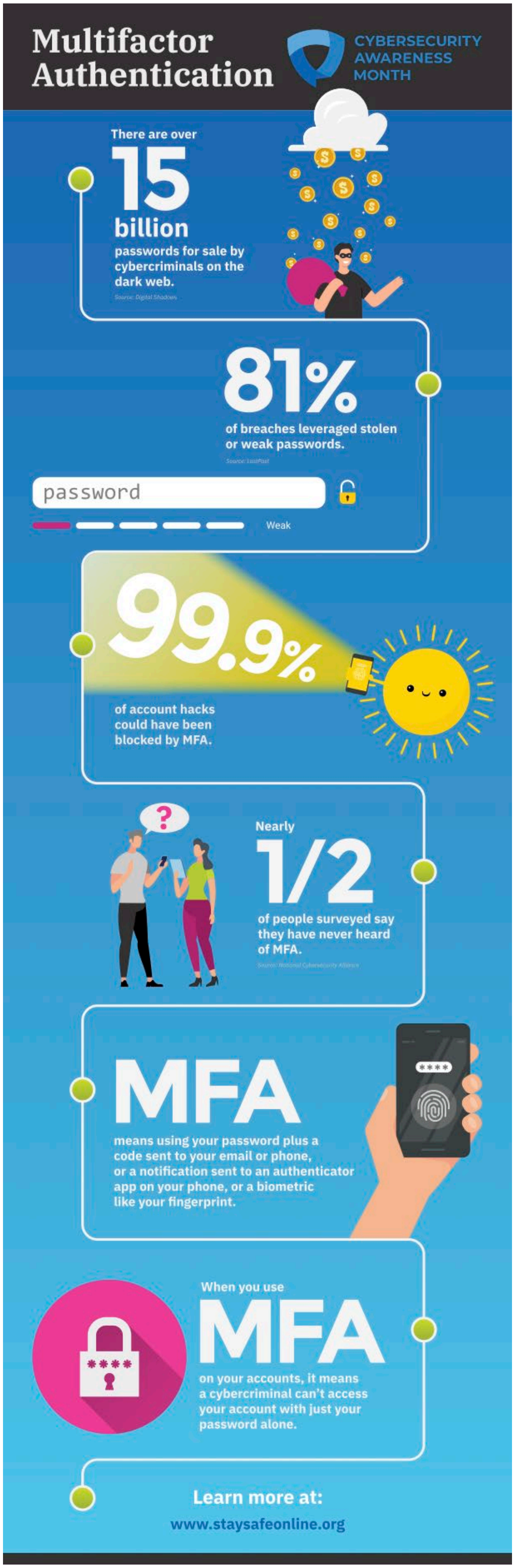
- **Apple App Store** (for iPhones and iPads) or
- **Google Play Store** (for Android devices such as the Samsung Galaxy).

Once the authenticator app is set up, when you log into your Microsoft 365 @ssndcp.org account you may select "**Approve a request on my Microsoft Authenticator app**," and an alert will appear on your smartphone or tablet. Select "approve" to verify your identity.

Watch out!: A common obstacle to authentication can occur when getting a new phone number or if you initially used someone else's phone number to set up MFA. If the prompt displays a phone number (the last two digits) that **do not** correspond with your correct phone number, you have two options:

1. Please visit the security verification page
2. Contact the help desk at 1-800-373-7521 or helpdesk@ssndcp.org

As frustrating as these steps may seem, it's vital not only to use multifactor authentication for your @ssndcp.org account, but to use it on all your personal accounts, including social media, email, and banking. We can't list every service you might use, but we encourage you to use it whenever the option is available!



Multifactor Authentication

CYBERSECURITY AWARENESS MONTH

There are over 15 billion passwords for sale by cybercriminals on the dark web.

Source: Digital Shadows

81% of breaches leveraged stolen or weak passwords.

Source: LastPass

99.9% of account hacks could have been blocked by MFA.

Nearly 1/2 of people surveyed say they have never heard of MFA.

Source: National Cybersecurity Alliance

MFA means using your password plus a code sent to your email or phone, or a notification sent to an authenticator app on your phone, or a biometric like your fingerprint.

When you use MFA on your accounts, it means a cybercriminal can't access your account with just your password alone.

Learn more at:

www.staysafeonline.org

Week 1: Cybersecurity Awareness Month - Multi-Factor Authentication (MFA)

Follow these links to enable MFA for: Apple ID, Gmail, Facebook, and Yahoo. If you use an email service that doesn't offer the option of MFA, we highly recommend discontinuing that email address and switching to a @ssndcp.org account.

For more information about using MFA, please refer to the following article: Setting up multi-factor authentication (MFA) on @ssndcp.org (Microsoft) accounts (ssndcentralpacific.org)

Please continue to follow along this month at our IT Resource Center where we will cover a variety of topics to help keep us safe in our digital lives!