Navigating the New Normal
Many now find themselves teleworking during the Pandemic. Working remotely supports public health efforts to reduce the spread of COVID-19, but it also presents new challenges for working securely. You can be certain that hackers are ready to seize the opportunity. The best way to protect your personal and professional information and systems accessed on your work devices, personal devices, and devices kids may be using for school is by using Multifactor Authentication (MFA).

What is MFA?
MFA, sometimes called Two-Factor Authentication or 2FA, is something you’re likely already using, like when you:

• Swipe your bank card at the ATM and then enter your PIN (personal ID number).
• Log into a website that sent a numeric code to your phone, which you then entered to gain access to your account.

MFA helps protect you by adding an additional layer of security, making it harder for bad guys to log in as if they were you. MFA/2FA requires you to present two or more pieces of evidence—your credentials—when logging in to a

Authenticating Yourself for Access
Your credentials include something you know (like a password or PIN), something you have (like a smart card), or something you are (like your face or fingerprint). Your credentials must come from two different categories to enhance security—so entering two different passwords would not be considered multi-factor.
When should I use MFA?
You should use MFA whenever possible, especially when it comes to your most critical devices—like your laptops, mobile phones, and tablets; as well as your sensitive data—like your work-related information systems, your work and personal email, all financial accounts, and your health records.

While some organizations require you to use MFA, many simply offer it as an extra option that you can enable. If the latter is the case, you must take the initiative to turn it on.

Furthermore, if a business you interact with regularly, like your health organization, wants to provide you with convenient online access to health records, test results, and invoices, but only offers a password as a way to protect that data, consider saying, “no thanks, not until you provide MFA to secure my information.”