J.P.Morgan

READINESS AND RESILIENCY

Are you prepared?

With all that’s happening around the world these days, it’s best to be aware, prepared and proactive.

FIVE WAYS TO PROMOTE READINESS AND RESILIENCY

❶ Prepare to work remotely

❷ Update your personal computers and devices

❸ Stay aware of your surroundings and don't fall for free Wi-Fi

❹ Secure your home Wi-Fi

❺ Remember: Scammers follow the headlines

For more information about safeguarding your operations, visit jpmorgan.com/technology or contact your J.P. Morgan representative.

GEOPOLITICAL UNCERTAINTIES. NATURAL DISASTERS. GLOBAL HEALTH CRISES. DATA BREACHES.

These are just some of the headlines we have all become so accustomed to. Being proactive is key to staying ahead and being prepared when these headlines hit close to home. Consider taking these five key actions to secure your home computer, personal devices, your online activities and physical workspace:

1. Be prepared to work remotely

Test your remote access capabilities so that you are able to work remotely if the need arises. If you have a company-provided laptop, bring it home (along with the power cord), and make sure your remote authentication tools are working.

Check to see if your company-provided “token” (e.g., Yubikey, RSA, Google Authenticator, etc.) is active and reset your pin if you have any trouble conducting your test.

These tokens enable multifactor authentication (beyond just a username and password) and add an additional element of security. If you experience any challenges with your remote access, contact your company’s IT Help Desk immediately.

You should also make sure you have all necessary company-approved applications installed on your company-provided devices.

2. Update your personal computers and devices

Always keep your operating systems, applications, and anti-virus software on all your personal devices (desktops, laptops, tablets, phone, etc.) up-to-date. If there is a patch or critical update available, then update that software immediately, and don't download applications that are not available via the official app stores (e.g., Apple, Android, Google stores, etc.).

(continued)

3. Stay aware of your surroundings and don't fall for free Wi-Fi

In the event you need to work remotely, only conduct business using company-approved applications and websites. Avoid working in crowded public spaces and do not conduct business over public Wi-Fi.

If you use Wi-Fi at home or another trusted location, then always confirm the network (SSID) name and never permit your device(s) to auto-connect. As an added layer of security, consider using a company approved Virtual Private Network (VPN) when accessing the internet.

4. Secure your home Wi-Fi

Ensure only authorized users can access your home Wi-Fi. Unlike physical networks, Wi-Fi systems can extend beyond the walls of your home. Therefore, you need to consider implementing important security measures that protect you from intruders.

Begin by securing your network by making your Wi-Fi password long and strong (e.g. 16 characters, with a combination of letters, numbers, and special characters), and limit the number of people who know the password.

You should also change the default user name and password of your router's administrator credentials, as many default passwords can be found on the internet. Finally, you should also ensure that you are using strong encryption such as WPA 2 or WPA 2 AES, and avoid using older encryption such as WEP and WPA.

5. Remember: Scammers follow the headlines

Do not believe everything you read online. Scammers like to capitalize on pandemics, natural disasters and other incidents to take advantage of their victims during a vulnerable time.

Ignore offers or advertisements pertaining to vaccinations, medical supplies like masks or hand sanitizer, urgent alerts or investment opportunities.

There are also fake malware websites (e.g. Live Coronavirus Maps) that appear to be legitimate, but actually infect your devices with malware to steal passwords and other information.

Be suspicious of unsolicited messages of any kind, including SMS messages and phone calls that may spark a sense of fear, urgency or curiosity.

Be aware of the signs of phishing (e.g. an email requiring urgent action, originating from a suspicious email address or linking to a suspicious website).

If you receive a suspicious email on your work account, report it immediately to your IT Security Department instead of ignoring, deleting or even worse, forwarding it to a colleague.

Only make donations to reputable sources. Ensure that the website is a legitimate donation site by double-checking the website address, and ensure the website is encrypted (e.g. website address begins with "HTTPS") before providing credit card or bank account information.

This document is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided in this document is intended to help clients protect themselves from cyber fraud. It does not provide a comprehensive listing of all types of cyber fraud activities and it does not identify all types of cybersecurity best practices. You, your company or organization are responsible for determining how to best protect against cyber fraud activities and for selecting the cybersecurity best practices that are most appropriate to your needs.

JPMorgan Chase Bank, N.A. Member FDIC. The products and services described in this document are offered by JPMorgan Chase Bank, N.A. or its affiliates subject to applicable laws and regulations and service terms. Not all products and services are available in all locations. Eligibility for particular products and services will be determined by JPMorgan Chase Bank, N.A. or its affiliates.