Remote Worker Update - Cybersecurity Guidelines for NJM Staff

Working from home at a time like this certainly helps in many ways. However, it's important to be aware of online security threats. Below are some tips to help you stay safe online so you can work remotely with peace of mind.

Home vs. public Wi-Fi networks

Most employees should be working out of their home where they can secure their Wi-Fi. When setting up your wireless router, be sure to configure it with a password. To do this, refer to your owner's manual or contact your internet service provider. Never leave your home Wi-Fi open and unprotected allowing anyone to connect. Also, you should always avoid using unsecured public Wi-Fi networks. Public Wi-Fi connections are often used by malicious parties to spy on internet traffic and collect confidential information.

Using personal devices and networks

Some staff members may be using their personal computer and Citrix to remote into their desktop at NJM. To keep your home computer and network secure:

1. **Install antivirus software** and turn on automatic virus definition (detection) updates.
2. **Enable automatic software updates** on your computer and devices, which will ensure that you are receiving the latest security patches.
3. **Create strong passwords -** Change default passwords to a strong password for all internet connected devices. This includes routers, smart TVs, game consoles, and anything that requires a login. Never use the same passwords for both work and personal accounts.

Be Aware of Coronavirus Scams

Many new scams are coming out related to the Coronavirus. **Malicious websites** have been created that appear to be Coronavirus maps and informational websites that can infect your computer with malicious software.

New Coronavirus **phishing emails** are also appearing. Here are some examples:

- Emails that appear to be from the CDC (Centers for Disease Control) or the WHO (World Health Organization), but actually contain malicious phishing links or dangerous attachments.
- Emails that ask for charity donations for studies, doctors, or victims that have been affected by the Coronavirus. Scammers often create fake charity emails after a global phenomenon occurs.
- Emails that claim to have a "new" or "updated" list of cases of Coronavirus in your area, which contain dangerous links and information designed to scare you into clicking on the link.

Always remember the following to protect yourself from scams:

- Never click on links or download attachments from an email that you weren't expecting.
- As always, if you receive a suspicious email, report it using the "Report Phish" button in the upper right corner of your Outlook tool bar.

For information on the Coronavirus, you should go directly to the official websites of the CDC (Centers for Disease Control) at https://www.cdc.gov or the WHO (World Health Organization) at https://www.who.int or you can also visit the NJ Department of Health website at https://www.nj.gov/health.