From The Office of Community and Economic Development

City of Long Branch

7 Tips To Help You From Being Hacked While Working Remotely

With all or most of us working these days remotely, we stand a higher chance of getting our files infected with some type of malware or phishing scam. To help prevent this from happening with you or your team, we listed a number of prudent tips below.

IRS Issues Warning About Coronavirus-Related Scams.

The IRS' Criminal Investigation Division has seen a wave of new and evolving phishing schemes. To help you or your team from getting taken, they should NOT provide their direct deposit or other banking information for others to input on their behalf into the secure portal.

Click Here To Read Norton's Article, "Coronavirus phishing emails: How to protect against COVID-19 scams."

The IRS reminds taxpayers that scammers may:

- Emphasize the words "Stimulus Check" or "Stimulus Payment."
- Ask the taxpayer to sign over their economic impact payment check to them.
- Ask by phone, e-mail, text, or social media for verification of personal and/or banking information, saying their information is needed to receive or speed up their economic impact payment.
- Suggest that they can get a tax refund or economic impact payment faster by working on the taxpayer's behalf.
- Mail the taxpayer a bogus check, perhaps in an odd amount, then tell the taxpayer to call a number or verify information online in order to cash it.

What Are Your Cyber Security Policies?

To minimize your company's exposure, we suggest training all employees (can be done with a webinar) on safe cyber-security

practices. That being said, we have listed several tips below to help keep your company's HR data safe.

1. Mandatory Cyber Security Workshops - To keep your team up to date on the cyber issues or phishing scams, consider creating a cyber-safety class for all employees.

2. Make Sure To Always Use A Strong Password - To ensure your team members are using a strong password, require the use of one uppercase letter, one number, and one symbol in their password, i.e., "Baseball@0601" versus "baseball" as a password.

3. Require Passwords To Be Changed - Train (or require) employees to use a strong password for each site visited and to change their password every 90-days.

4. Teach Team Members About Phishing Scams - To prevent an employee from opening an attachment or e-mail from a hacker, you should educate them on what a "phishing scam" looks like when it arrives in their inbox.

5. Install A Password Management System - The most common passwords are "password" "123456," "12345678," and "1234." A good password manager can help eliminate this issue by creating an ultra-strong password every time an employee visits a website.

6. Block File Types That Often Carry Malware - Block executable file types from being received by e-mail or downloaded from the Internet.

Executive Summary: As your staff accesses their e-mail and/or company files via mobile or tablet devices, it just opens up gateways to hack your company's employee data. IT professionals know they cannot fight this battle alone. That being said, it is imperative for your HR department and staff to know what to look for in this ever-changing landscape.