Nationwide®
is on your side

Work-from-home resources

Cybersecurity tips

Stay secure when working from home

We understand there are new challenges you're facing today as you work from home, including increased cybersecurity risks. To help you protect your network, our Threat Intelligence Advisory team would like to share these insights and tips to avoid cyber risks.

Overview

The COVID-19 pandemic, and the resulting pivot to a work-from-home (WFH) environment for many of us, provides an attractive opportunity for cyber threats to occur. Nationwide® has observed phishing attacks—fraudulent emails that come from seemingly legitimate sources used to persuade you to reveal sensitive personal information—that leverage the fear, uncertainty and doubt associated with the virus threat. We anticipate these attacks will continue for the foreseeable future.

Opportunistic attacks

The volume of coronavirus-themed phishing and social engineering campaigns, designed to manipulate people into divulging confidential behavior, has increased steadily from initial reports observed early this year. The attacks can be placed into three main categories:

Email scams delivering malware and fake mobile apps

The sale of fake or counterfeit goods offering deals on medical supplies, etc.

Social media misinformation designed to create panic

Remote support scams, particularly the fake IT support variety, may also increase as scammers lean on the knowledge that people not accustomed to working remotely could be encountering system issues as part of their WFH transition.

Expansion of attack surface

An "attack surface" is the total number of points an unauthorized user could exploit to gain access to your system. Adversaries may be able to take advantage of an expanded attack surface made possible by the WFH environment. These may include:

- Unsecured "internet of things" (IOT) devices such as security systems, thermostats and electronic appliances
- Unpatched home computers
- Phishing campaigns directed against personal email accounts

The significant increase in the number of people doing more work via web browsers opens your business to the risk of browser-based attacks via malicious plug-ins and web-based exploit kits. Additionally, scammers may look to ramp up identity attacks because their malicious network traffic and signaling stands a better chance of staying hidden among the expected increase in legitimate remote traffic.

Our recommendations

To address the increased risks associated with working from home, we recommend continuing to practice good security habits enforced on your office network, particularly around social engineering scams and phishing attacks. Unfortunately, these good security habits don't always carry over from the office, as we tend to let our guard down at home (i.e., writing down passwords, leaving sensitive information lying around or leaving devices unlocked).

Tips for securing home networks and IOT devices

Secure your home wireless (Wi-Fi) network
Be sure to change the default admin password, enable WPA2 encryption and use a strong password for your Wi-Fi network.

Be aware of all devices connected to your home network
This could include smart thermostats, gaming consoles, baby monitors, TVs, appliances and possibly even your car. Make sure they are protected with a strong password and have had all system updates applied.

Keep your operating system and your applications patched and up to date
Whether you're using Windows or macOS, making sure to update your software regularly is important. If automatic updates are an option, be sure to enable them.

Make sure each of your accounts has a separate, unique password
Also consider using a password manager to securely store your passwords.

We're here for you

Nationwide is committed to providing you with the support and resources you need as we navigate today's challenging economic and market conditions together. We appreciate your partnership and the opportunity to work with you.

Resources

https://www.sans.org/security-awareness-training/resources/smart-home-devices

https://threatpost.com/working-from-home-covid-19s-constellation-of-security-challenges/153720

https://www.sentinelone.com/blog/covid-19-outbreak-employees-working-from-home-its-time-to-prepare

For financial professional use only, not for use with the public

Nationwide®