Are You Operating in a Secure Remote Work Environment? Review These Cybersecurity Measures for Home

Description

With the remote workforce rapidly increasing over the past dozen years, and more companies coming to terms with the necessity of employees working remotely, there is much to consider regarding managing a successful remote team. A remote workforce demands an entirely different structure than operating in a multi-person, shared office environment. It calls for a fresh approach to management, new cost considerations and implementation of specialized tools, as well as different approaches to cybersecurity, closer attention to time management, and the creation of virtual and physical environments conducive to motivation, stimulation, collaboration and focus.

In a report issued in February 2020 â?? just prior to a massive upsurge of remote workers due to the COVID-19 pandemic â?? FlexJobs, a career search and recruitment company, and Global Workplace Analytics released the following findings:

â?¢ From 2016-2017, remote workers in the United States grew 7.9 percent;
â?¢ In the last five years, the remote workforce grew 44 percent;
â?¢ In the last 10 years, the remote workforce grew 91 percent; and
â?¢ Between 2005 and 2017, there was a 159-percent uptick in U.S. remote workers.

The dramatic growth is the result of remote work becoming increasingly attractive to cohorts that are focused on health, work-life balance, business continuity, cost savings, productivity, the environment and having access to a larger talent pool.

According to Jason Fried and David Heinemeier Hansson, creators of web-based project management tool Basecamp, an employeeâ??s commute alone, to and from work, negatively impacts many of these factors. They noted research conducted by Slate Magazine, which found that commuting is associated with an increased risk of obesity, high blood pressure, heart attacks, depression and divorce. In addition, time spent commuting reduces the number of hours available to work, be with family and friends, conduct personal business or enjoy leisure activities.

While the benefits are appealing, working remotely doesnâ??t come without its challenges. One challenge is avoiding the pitfalls of a cyber attack. Here are some cyber insights and tips for real estate professionals who are managing remote teams or have recently made the shift to working remotely.

Cybersecurity Checkup

During a crisis, criminals look for weak areas to infiltrate. With the swift shift of many employees in the business world to a remote work environment, fraudsters are taking advantage of the chaos and stress of the transition. There are specific things you can do to mitigate cybersecurity threats and enable a secure workplace at home. The SANS Institute, a research and education provider for security professionals, shared these five simple steps to mitigate vulnerabilities:

Five Cybersecurity Tips for Home

1. Be aware of and vigilant against increased social engineering scams. Scammers have learned that the easiest way to get what they want is to target you, rather than computers and devices.
2. Secure your home Wi-Fi network.

Change the default administrator password, make it a strong password, and only allow people you trust to be on it.

3. Practice good â??password hygiene.â?• Create strong passwords: The more characters a password has, the stronger it is. Use a password manager, which is a specialized program that securely stores all your passwords in an encrypted format. Enable two-step verification (also called two-factor or multi-factor authentication) whenever possible.
4. Make sure each of your computers, mobile devices, programs and applications are running the latest version of their software. To stay current, simply enable automatic updating whenever possible.
5. Make sure family and friends understand they cannot use your work devices. They can accidentally erase or modify information, or, perhaps even worse, accidentally infect the device.

Added Protection

The FBIâ??s Internet Crime Complaint Center (IC3) reported 791,790 complaints of suspected internet crime in 2020, an increase of 69.4 percent from 2019. Reported losses totaled $4.2 billion, up from $3.5 billion in 2019. The agency recommends the following measures:

â?¢ Do not provide your username, password, date of birth, Social Security number, financial data or other personal information in response to an email or robocall;
â?¢ Always verify the web address of legitimate websites and manually type them into your browser;
â?¢ Check for misspellings or wrong domains within a link; and
â?¢ Do not open attachments or click links within emails from senders you donâ??t recognize.

On a recent remote workforce cybersecurity webinar hosted by NATIC, Chris Gulotta, founder of Real Estate Data Shield, and Ryan Cabrita, information security officer of Real Estate Data Shield, recommended employers configure a virtual private network, or VPN, so employees are relying on the office network as opposed to their individual network. This provides more security to the companyâ??s assets and allows the employer to monitor activity on the network. In addition, if employees are using their personal phones for business use, Cabrita advised to restrict their use to emails only.

Zoom Security

IC3 also advises remote workers to carefully consider the applications used for teleworking, including video conferencing software systems.

â??Malicious cyber actors are looking for ways to exploit telework software vulnerabilities in order to obtain sensitive information, eavesdrop on conference calls or virtual meetings or conduct other malicious activities,â?• IC3 said.

Cabrita recommended paying for Zoom Pro or Zoom Business in order to have access to features that provide enhanced security and control over the platform. He advised to always require a password for Zoom meetings and to save any recordings locally and remove them from the Zoom cloud.

â??If you remove [the recording] and save it locally to your office network â?¦ youâ??re reducing the risk,â?• Cabrita said. â??Not only should you remove it from Zoom, you also need to remove it from Zoomâ??s Trash, like the equivalent of the recycle bin in Windows.â?•

After purchasing a Zoom plan, you can log in to your administrative account, and under the Advanced/Security section, you can read through each option and make an informed decision about each feature.

Five security tips for Zoom meetings and webinars:

1. Always require a password.
2. If recording, create a recording advisory to participants.
3. Enable the waiting room.
4. Restrict screen sharing.
5. Restrict who can download the recording.

Following these tips will not only help your remote employees succeed, but ensure they do so in a cybersecure way. Schedule regular check-ups to make certain these concerns remain a top priority for your company.

Kelly McCarel
As Vice President of Education and Content for North American Title Insurance Company (NATIC), Kelly McCarel delivers relevant information title agents need to achieve their business goals and remain compliant with state and federal laws. She brings nearly 20 years of experience as an education, marketing and communications professional to her position. Prior to joining NATIC, Kelly served in multiple leadership roles at October Research LLC, an award-winning multimedia publishing company serving the real estate, settlement services and mortgage lending industries. Previously, she managed a diverse platform of marketing and communications programs for an international healthcare company and developed educational and news content for several legal and real estate publications. She has focused her career on developing marketing and educational strategies using various forms of digital and print distribution platforms; promotional campaign production and management; content development; public relations; B2B journalism; and seminars and webinars.

Category

1. Cybersecurity
2. Featured
3. Uncategorized

Tags

1. featured

Date Created
2021/06/23
Author
vltaexaminer