Remote Work and Scammers

Companies invest small fortunes in their IT security.

Firewalls, virus and malware scans, hardened servers, air gapped systems, even personal instruction on best practices all help to keep critical infrastructure safe from the near-constant threat of external attack. Some high-profile institutions, such as banks, law firms and national security agencies, consider these measures so essential that they refuse to allow certain work from home altogether.

Many of those rules have fallen by the wayside as workers scatter to home offices during the coronavirus quarantines. The law firm Mintz, Levin noted the risk this can cause in a March article for the National Law Review. Watching the nation-by-nation quarantines coming, they wrote that "while remote working arrangements may be effective to slow the community spread of COVID-19 from person to person, they present cybersecurity challenges that can be different than on-premise work." Those challenges are here, and they're far from theoretical.

By Yoav Keren, BrandShield CEO

Apr 2020

Challenge #1: Out of Office Communication

Remote workers have come to depend on asynchronous communication to an unprecedented degree during the coronavirus quarantine. They are accessing their work through web portals and often communicating intensively over e-mail and social media. Yet at the same time, one of the most essential elements to any corporate security system is employee vigilance when it comes to those exact same systems.

Your employees need to be scouring incoming messages, whether over social media or e-mail, at a time when they receive more than ever. More than that, under ordinary conditions they would know to suspect any message asking for sensitive information or sending an unsolicited attachment. Yet with the world working from home, sensitive information now moves entirely through inboxes and many employees depend on corporate social media for updates and workplace announcements.

Meanwhile, your staff gets up every morning and logs into the corporate VPN, multitasking their new routine alongside making coffee, checking the headlines and trying to keep one eye on the kids. As long as the site looks right, with logos and layout in the right place, scammers count on the fact that out of every, single employee logging in every, single day, at least a few of them won't notice that the URL begins with "http" instead of the all-important "https."

The Attacks Have Already Begun

Even during ordinary workdays an organization's personnel are its biggest weak point, from the C-Suites to the lowest paid employees. Hackers try to take advantage of human error through scams such as fraudulent social media accounts, faked web pages and online phishing, all of which target your employees both at and away from the office. One prominent hacker group has even become known for targeting workers exclusively at hotels while on business trips, taking advantage of remote work to steal data.

Those attacks have not waned, but security experts have also identified new varieties of scams in the wake of the coronavirus quarantine. Many take advantage of the specific security challenges created by workers logging on to their office systems from unsecured home environments. While working from home creates many new challenges, it's important to highlight four in particular:

Challenge #2:
Web Portals

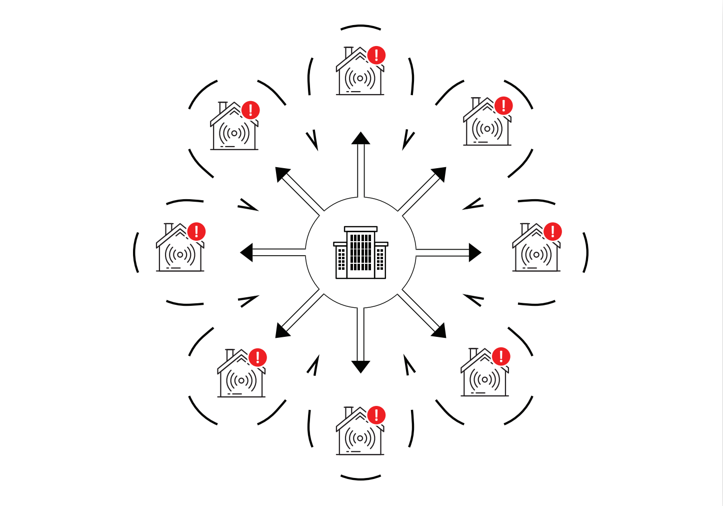
In the wake of the coronavirus, “Zoom” has become a verb. Arguably not even Amazon has enjoyed as much success and growth as this, formerly niche, video chat company.

With that growth has come risks.

Many video chat and other remote communication tools were not necessarily built with security in mind. Offices use these suites because they emphasize collaboration and seamless communication, but that easy transfer of information has also created opportunities for hackers.

False links now proliferate, with invitations to meetings that claim to be from a company leadership, corporate groups or customer-facing PR teams. In other cases, hackers and even simple vandals can get ahold of legitimate links to your corporate events. In particular the problem of “Zoombombing” has become a well-known phenomenon during the quarantine. During this form of vandalism, individuals get ahold of a link and jump in on a private video call. Often they behave disruptively, broadcasting explicit images or otherwise making it impossible to work. Sometimes they try to lurk in the background and gather sensitive information.

At best, you may be left trying to rebuild from an embarrassing incident in front of a customer or client. At worst, you may have to figure out how that internal document became public.



Challenge #3:
Off Campus Networks

Moving an entire workforce out of the office creates problems. As the security law team at Jones Day notes, it has forced corporate IT staffs to split their attention among different needs when social distancing has left them with reduced capacity already.

At the same time, your employees have begun conducting business in a far more vulnerable environment. Home networks operate without the firewalls or layers of security that help keep an office environment secure even from successful attacks.

Your office network can protect itself when a user does download a malicious file or enters the information into a spear phishing site. A basic Linksys router cannot.
For a hacker, this means that home networks have become a prime target. Instead of scamming their way into a hardened corporate system, they can hijack barely-protected personal networks. Your servers will expect that remote login, and may not be able to tell the difference between a member of your legal team and a hacker using that employee’s wireless network as their very own VPN.

Challenge #4: Personal Devices

How many of your employees allow their children to use their personal laptops? How many are careless about the files they download or websites they visit? How many have kept their antivirus and malware protections up to date? How many simply click away the pop-up box that prompts them for updates?

There's a reason your IT team stays so vigilant when it comes to the hardware and software around the office.

While some firms have sent employees home with dedicated laptops and other devices, many employees now rely on their personal computers and smart phones to do remote work. These devices have an order of magnitude more security concerns, all of which your IT team can't address without physically inspecting and overhauling every, single laptop currently logging on to your network. We don't recommend this.

Personal devices create a serious risk for your workspace. As with home networks, they lack the technical layer of security that protects your information if a scammer does manage to deceive employees and install malicious software on their computers. Worse, they have many more points of potential vulnerability.

In a dedicated office environment your employees will conduct some personal business, but now the same machine processing their professional data also handles all of their personal conduct. Scammers can attack them through falsified corporate websites and by posing as colleagues, but also through every fake tech support Twitter account, fraudulent Facebook message from an "old friend," and malware infested download that can hijack an employee's computer during their down time.

And, now, the keyboard capture program that they unwittingly install will also capture every word of confidential information they write while logged on to the corporate server.

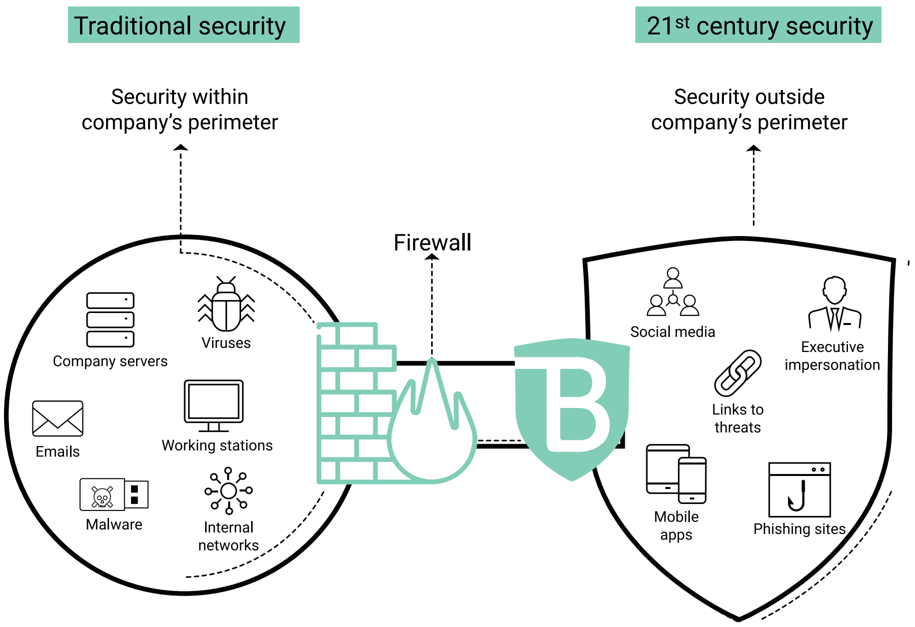
The Best Defense Is a Good Offense

The truth is, there's only so much your IT team can do to help keep your information safe in this environment. The threats are coming at them fast, at a time when they are already trying to keep up with user demand for daily services.

Instead, one of the best ways to protect your information in a distributed work environment is to look outward. Your employees are scattered across the world and throughout the internet, which is where your attention has to be as well. Search vigilantly for anyone attempting to create websites that mimic your corporate brand or presence, and particularly look for any that attempt to duplicate internal login screens. Constantly monitor for URL strings similar to your own intranet and VPN login addresses, any which might result from easy typos, as well as for any sites that use your corporate logo, trademarks, slogans or other identifying features.

At the same time, monitor social media sites for profiles that mimic your company or its brand. Look for accounts claiming to post official announcements or targeted at your employees or customers, once again searching for substantially similar user names, branding, imagery, trademarks or corporate slogans.

Traditional vs. Proactive Security Perimeters



Finally, train your employees to pay attention to their daily routines.

Empathize and emphasize: Empathize with what they're going through right now, as many will be having to split their attention between duties to work and families, while at the same time emphasizing the need for additional caution in the current environment. Distribute direct links to critical websites, such as logins for intranets, and encourage them to access those sites by clicking the official links rather than attempting to enter the URL from memory. And periodically remind your work force of best practices.

This will require attention over the long haul, and it won't help to get frustrated when your employees forget about an e-mail that IT sent them weeks ago.

That all may sound like a lot, but the good news is that we here at BrandShield can help. Our team of experts has seven years of experience protecting our clients' identity on the world wide web. We detect online counterfeiters, whether they have stolen your identity on social media or duplicated your corporate websites. Then we work with domain registrars, web hosts, social media companies and online marketplaces to take the frauds down.

The best way to stop an attack is before it starts. We can help you make sure that you find that fake intranet login long before a single employee does.