BrandShield

COVID-19: As Fear Spreads, so Do Scams

For scammers and con artists disaster is simply another word for opportunity. A crisis means desperate, frightened consumers, overwhelmed corporations, and security professionals distracted by their duties both at work and at home. They exploit security vulnerabilities when transitioning to **remote work** for most employees.

—

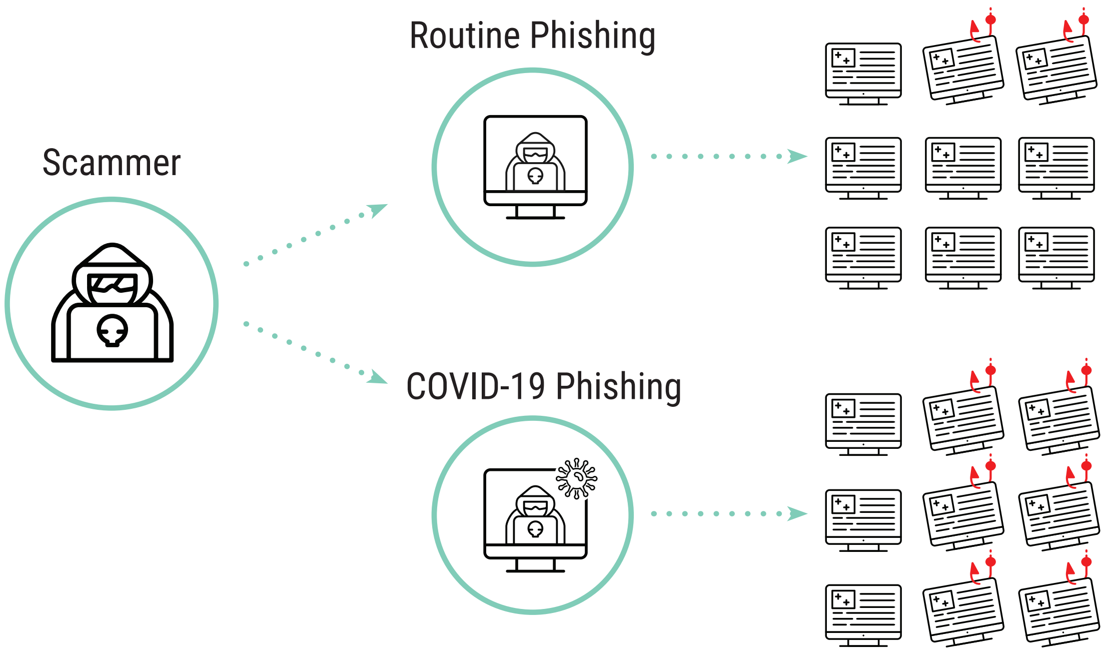
By Yoav Keren, BrandShield CEO

Apr 2020

COVID-19 Phishing Has Taken Off

Almost immediately after the COVID-19 outbreak began to make headlines, security professionals around the world flagged the first digital fraud based on the novel virus. As the Electronic Frontier Foundation notes in its alert on COVID-19 scams, "mentioning national headlines can lend a veneer of credibility to scams. We've seen this tactic time and time again, so it's no surprise that COVID-19 themed social media and email campaigns have been popping up online."

Current emotions magnifies the damage that a scammer can do to you



Since then fraudulent social media, websites and e-mails have grown so quickly that the United States' Federal Trade Commission has dedicated a web page to the subject.

This creates a new and increasingly dangerous environment. As attacks proliferate, they take advantage of the public's trust at a time when consumer emotions run high. This magnifies the damage that a scammer can do to your reputation. It's bad enough to have someone steal your name to run a tech support scam or request client information. It's much worse when "your company" tweets out an alert promising to flag ATM's exposed to the COVID-19 or when a criminal grabs pictures of your executives to build their COVID-19 diet plan website.

Fortunately, you can act to protect yourself and your company from this threat.

What Are They Doing?

Remote Work Related Phishing

Customer Facing Phishing

Social Phishing

Online Impersonation

Online Fraud

Scammers have taken advantage of the COVID-19, and the ensuing quarantines, to target consumers and companies alike.

As some outlets have explained, COVID-19 scams largely mirror traditional online attacks. Wired Magazine first reported on them as early as January, when outlets first began reporting on the new virus emerging from China, but hackers dramatically escalated their activities in March, when the virus began to dominate the news.

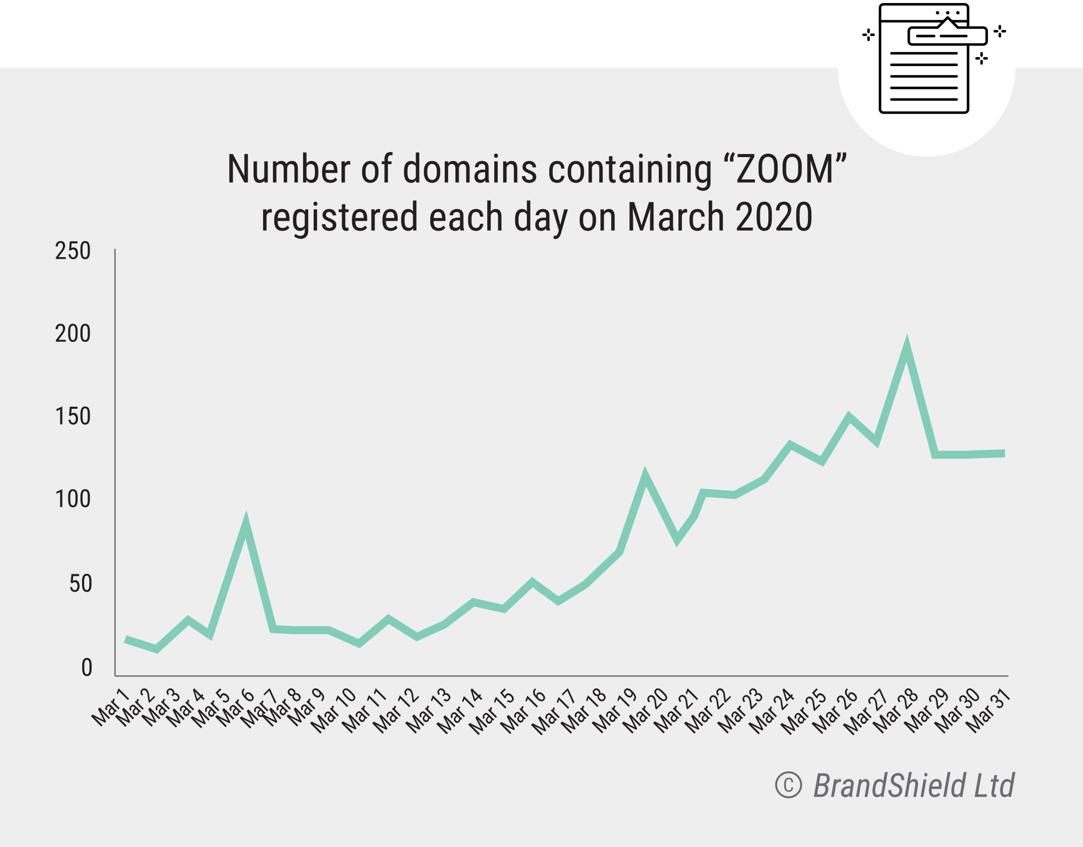
As with a traditional online scam, COVID-19 attacks promise the target something that they need, trust or want.

Some scams focus on consumers, posing as a critical source of information, a source for medical or personal necessities, or simply a new solution to emerging problems. For example, the FBI tracks fraudulent health and safety bulletins about COVID-19 in local communities or worldwide. Other scammers have created websites and social media accounts promising to sell masks and hand sanitizers. Some have even created phony networks offering short term loans for anyone left unemployed by the quarantines. All of them end in an attack.

Other messages go to work on a company's internal defenses.

In ordinary times your workers have the protection of your company's firewall and, often, an on-site IT team that can help them protect their data. Today those workers have been scattered. They're in their living rooms, far from the protections of a secured network and often using their personal (highly insecure) machines.

These scams run attacks we have seen in the wild many times before. Hackers will create social media profiles or e-mail accounts posing as colleagues or managers, pretending to send internal messages. These messages will often ask for routine information or claim to offer updates on key subjects such as corporate sick leave and work from home policies, material that your employees not only need but may be specifically expecting. Except, instead of a useful pdf, your employees download a ransomware packet.



Number of domains containing "ZOOM" registered each day on March 2020

© *BrandShield Ltd*

Why Is This Happening Now?

In a word, chaos. COVID-19 scams take advantage of the fear and confusion spreading around the world right now.

The truth is that even in good times, a vigilant user base helps against phishing, spear phishing and social media attacks. People need to look carefully at the messages they receive, and for an ordinarily overwhelmed workforce that's a lot to ask. With those same people stuck at home and bombarded by news on a daily basis, it's that much harder to examine their inbox.

What's more, your customers and employees are actively looking for these messages.

Individuals around the world, many in communities under quarantine, are under enormous stress. They want to know everything they can about this virus, their restrictions and updates on a quickly changing situation. They want news on test kits and vaccines. They're terrified for their financial future, and worried that any e-mail could be the next layoff notice. More than anything else, they want any sense of when this crisis will pass. To take advantage of that, criminals hijack your authority.

The tactics are straight out of a phisher's handbook. Criminals fake social media profiles, websites and spoof e-mail accounts. They will copy brand logos and identifying marks, and duplicate the exact look of an organization's social media pages and websites. They do everything it takes to make it look like a message came from a legitimate outlet because that's exactly what they want consumers to believe.

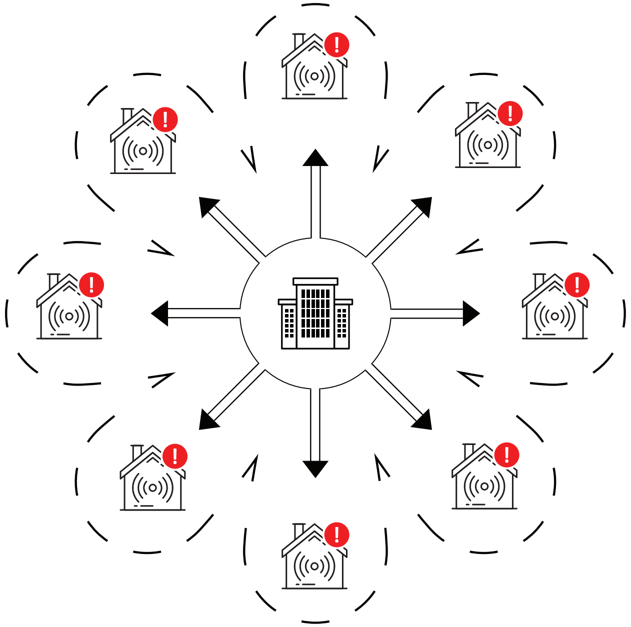
Some common attacks claim to be from public agencies such as the Centers for Disease Control or the World Health Organization. Others steal the identities of major charities and companies. The Electronic Frontier Foundation, for example, has posted sample e-mails it got from hackers posing as the Gates Foundation and a major university.

Still more spoof brands and health care institutions. Security professionals report e-mails claiming to represent companies offering products that will help during the COVID-19 outbreak, everything from fake charities and student debt forgiveness to hand sanitizer and in-home ventilators. It's common for these attacks to hijack companies and well-known brands because customers look for their information from these sources. When their local bank reaches out offering financial help, they're not just ready to believe that it's real.

With people stuck at home and bombarded by news on a daily basis, it's that much harder to control.

What Should You Do?

Remote Work
External Protection Layer Required



It's important to remember that whether or not your company gets hacked directly, you're no less under attack. Although with many workers working remotely, including in many industries that have typically banned VPN and offsite access for security purposes, the risk of a direct hack is greater than ever.

When criminals send out messages in your name claiming to offer lifesaving drugs, important products or essential information, the general public will quickly associate your company with these scams. Many won't separate the company from the scammer. They'll only remember your company as the logo on top of the message promising them a fake COVID-19 cure. And it only gets worse if that message winds up on the news.

That means you need to act.

First, follow the example set by organizations like the WHO. Send a message to your customers and employees warning them about the dangers of COVID-19 scams and the damage they can cause. Remind them that you will never ask for sensitive information in a blanket e-mail, and update them on the basic security measures they should take when working online. Duplicate that warning on your website.

Second, make sure that every one of your company's employees gets educated on the dangers associated with remote access. The goal is not to frighten already frightened people, but to remind your employees that now is a time to be more vigilant than ever, not less.

Third, actively monitor social media and the internet for bad actors posing as your company. While most security alerts focus on the dangers posed by e-mail phishing, the reality is that social media attacks are the fastest growing form of online scams out there. In the COVID-19 era, criminals rely on websites such as Facebook and Twitter more than ever to spread their malware and lies. That's a problem, but it's also a solution. It means you know where to look.

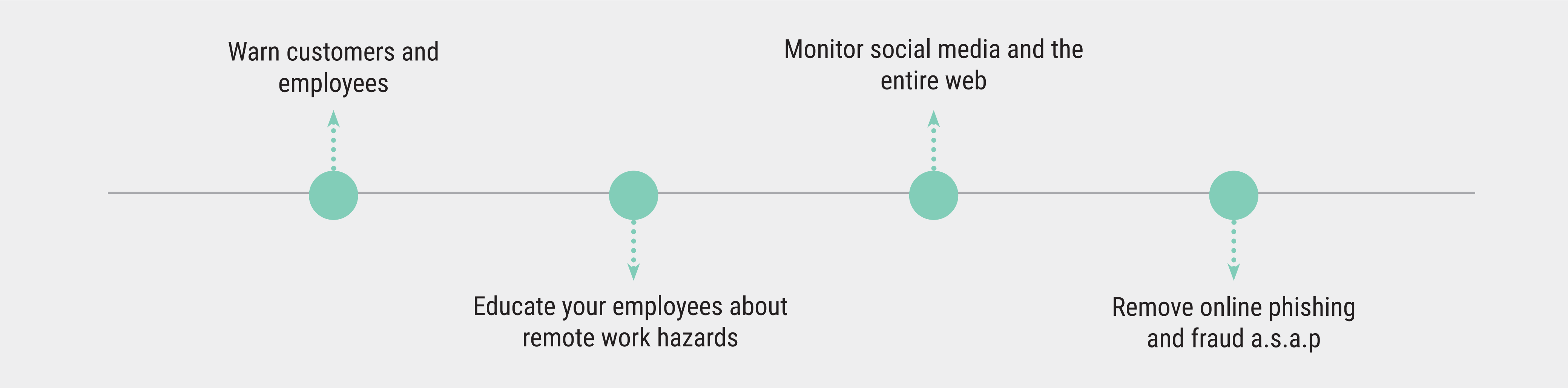
Don't let your customers or employees be the first ones to find a scammer posing as your HR manager or the brand outreach team you didn't know you had. Actively search social media for key concepts such as your company's name, logos, slogans, trademarks and even (when practical) your principal employees. All of these will help you find fraudulent accounts.

Finally, when you find a bad actor, you need to stop them. Immediately.

With many workers working remotely, the risk of a direct hack is greater than ever.

BrandShield can help with that. Relying on a team of technical and legal experts, as well as a web of relationships across the industry, BrandShield is well positioned to help you find and eliminate threats to your company and reputation. It isn't enough to know the criminals are out there. You need them taken down.

We can do that together.



Warn customers and employees

Educate your employees about remote work hazards

Monitor social media and the entire web

Remove online phishing and fraud a.s.a.p