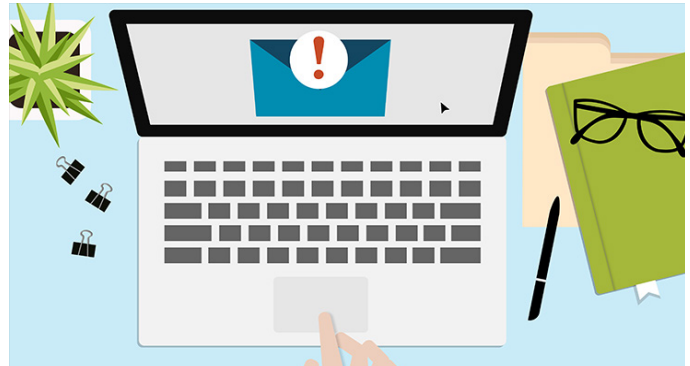


## Shark Tank Star Barbara Corcoran Loses Almost \$400,000 in Email Scam

**The detail that no one caught was the email was misspelled by one letter, making it the fake email address setup by the scammers.**



“Shark Tank” star Barbara Corcoran was reportedly taken for almost \$400,000 after her office was the victim of an email phishing scheme.

According to People, the 70-year-old mogul’s bookkeeper received an email about an invoice to approve a payment on a real estate renovation, which isn’t at all uncommon given how many real estate deals she works with on a daily basis. However, this one wasn’t legitimate.

“I lost the \$388,700 as a result of a fake email chain sent to my company,” Corcoran told the outlet. “It was an invoice supposedly sent by my assistant to my bookkeeper approving the payment for a real estate renovation. There was no reason to be suspicious as I invest in a lot of real estate.”

A representative for Corcoran told Fox News the star will not provide further comment on the matter at the advice of her attorneys until authorities are done with their investigation.

People reports the bookkeeper continued to correspond with the scammer, who was able to pretend to be the “Shark Tank” star’s assistant thanks to a clever deception involving the name of Corcoran’s actual assistant.

“The money was wired to the scammer yesterday and my bookkeeper copied my assistant, who was shocked to see her name on the correspondence. The detail that no one caught was that my assistant’s email address was misspelled by one letter, making it the fake email address set up by the scammers,” Corcoran explained.

It wasn’t until the bookkeeper sent a followup on the transaction to the actual assistant that they realized they’d been had. Unfortunately, by the time they realized what was going on, the scammer had already made off with the money that was mistakenly wired to them.

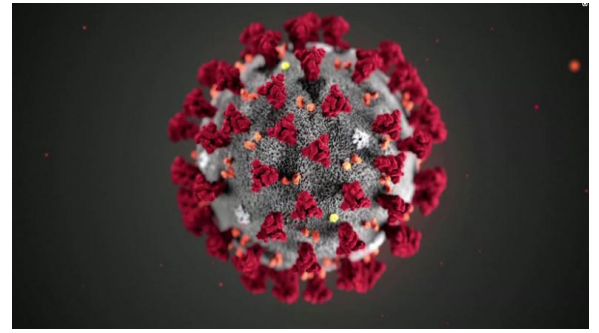
“The scammer disappeared and I’m told that it’s a common practice, and I won’t be getting the money back,” Corcoran told People.

She added: “I was upset at first, but then remembered it was only money.”

According to TMZ, the scammer pretended to be with FFH Concept GmbH in Germany, an actual company that Corcoran works with. It notes that her IT people reportedly traced the original emails to a Chinese IP address.

March 2020

## Coronavirus Scammers Are Seeking to Profit Off the Deadly Virus



The new coronavirus has been a bonanza for scammers and spies, who are exploiting the global thirst for information about the outbreak to make money and steal information, government officials and cybersecurity experts say.

Criminal hackers, scammers and even governments have been sending fake coronavirus-themed emails designed to trick people into opening attachments that download malicious software, allowing access to their data, experts told NBC News. Some messages have impersonated the World Health Organization and the Centers for Disease Control and Prevention, while others have masqueraded as communications from health authorities in other countries, including Ukraine, Vietnam and Italy.

The FBI is tracking so-called phishing campaigns that seek to use people's interest in the coronavirus to get them to click on links that encourage them to reveal sensitive login information, a top FBI official said.

"One of the things that's most concerning to us are phishing scams with a coronavirus theme," said Herb Stapleton, a section chief in the FBI's cyber criminal section. "This is a vector or an approach that we didn't see three months ago and now is suddenly successful." People can report bogus emails to the FBI by going to [www.ic3.gov](http://www.ic3.gov), Stapleton said.

The coronavirus phishing scam, which has been around since early February, has targeted users around the world. Police departments from Australia to the U.K. have issued warnings to be on the lookout for it. The WHO also issued its own guidance making it clear that it would never "ask you to login to view safety information."

A newer and lesser-known scam has recently been uncovered: emails purporting to be from CDC doctors and U.N. officials that encourage users to download malicious files. "A must read," says one bogus email purported to be from a CDC doctor, which the company showed to NBC News. "Find in the attached everything you need to know about the spreading and management of the deadly Wuhan Coronavirus..."

If a person clicks on one of the attachments promising guidance on how to "help prevent the coronavirus," malware will be downloaded onto the unsuspecting user's device. One malware package, called "Trickbot," typically tries to steal banking credentials, and the other, named "Fareit," which can log a person's keystrokes, typically tries to steal any and all login credentials.

Cybercriminals "recognize that when there is a crisis, people are hungry for information — they are looking for whatever is new," said Shawn Henry, who once headed the FBI's cyber division and

now works for a security firm, CrowdStrike.

"When people are hungry for information, they are vulnerable, because they've got their guard down."

CrowdStrike and other leading cybersecurity firms say the coronavirus has become the top new theme in schemes that use social engineering to induce recipients to open attachments or click on links that then open their computer files to attackers.

"This is dominating cybersecurity right now," said Jim Yacone, a former senior FBI official now at the SANS Institute, a cybersecurity research and education organization.

Security firm FireEye documented a China-based effort to extract information from Vietnamese government officials, as well as multiple campaigns targeting Ukrainian officials. The U.S. Secret Service said in a statement warning the public: "Coronavirus is a prime opportunity for enterprising criminals because it plays on one of the basic human conditions ... fear."

"Fear can cause normally scrupulous individuals to let their guard down and fall victim" to scams, the statement added.

The scams go well beyond the U.S. The security firm Fortinet found an email written in Italian, posing as a message from an Italian health agency, that induced users to click on an attachment that looked like a Microsoft Office document.

In fact, the user was downloading Trickbot malware.

Other hackers are sending emails with what purports to be a secret cure for the coronavirus. When recipients click on the link, they are asked to enter their credentials, according to the security firm Proofpoint, which also found fake WHO emails.

The FBI, the Secret Service and security firms urge people to:

- Avoid opening attachments and clicking on links within emails from senders you don't recognize.
- Always independently verify that any requested information originates from a legitimate source.
- Refuse to supply login credentials or financial data in response to an email.
- Visit websites by inputting their domains manually.

"Making the public aware of how to protect themselves is a really important step in stopping this type of activity," Stapleton said.

Source: NBCNews.com

# BEFORE THE BREACH

HACKERS ARE HERE!

NEW SKILLS FOR A NEW FIGHT

- 1 in 5 businesses will suffer a cyber breach this year
- 81% of all breaches happen to small/medium sized businesses
- 66% of companies do NOT test their backups
- 60% of companies that lose their data will go out of business within 6 months
- 92% of malware is delivered via email
- 97% of breaches could have been prevented with today's technology

Want to learn more about how to protect your business?

Stay tuned for our next lunch and learn date!



[www.preferreditgroup.com/beforethebreach](http://www.preferreditgroup.com/beforethebreach)



talk nerdy to me

## PREFERRED IT EMPLOYEE SPOTLIGHT



Meet Amy Horne! Amy is the wife of Preferred IT Group's CEO Jason Horne. She joined the Preferred IT team formally in August of 2018. Previously she worked as a controller for an environmental company for over 18 years. When Preferred IT began operations over 15 years ago, Amy helped with the accounting. She has always been part of the PITG team at heart! Amy has enjoyed her position working at Preferred IT. She gets to now do more than just accounting. She works on marketing and helps with dispatching, along with her accounting duties.

Outside of the office, Amy is in full Mom mode most of the time. She is a proud mother of three who always keep her on her toes. She gets to enjoy helping out in their classrooms and volunteering for their events. She goes between dance and softball for her two girls to football, wrestling and baseball for her son. There is never a dull moment in the Horne household!

When Amy isn't busy being a Mom, she enjoys time with her friends, weekends at the lake, reading, binge watching shows, and of course shopping! She also enjoys traveling with Jason and hopes to do more of that when her kids are grown.

## Apple is experiencing a shortage of replacement iPhones due to coronavirus

Apple has informed its tech support retail employees that stock of replacement iPhones will be strained for the next few weeks, according to Apple Store employees who spoke with Bloomberg. This shortage marks one of the first instances of the ongoing coronavirus outbreak and its many ripple effects on industries worldwide, affecting the iPhone maker's existing product supply. Bloomberg notes that the company's iPhone 11 and iPad Pro lines are beginning to see shortages as well. The company shared in a recent investor call that it does not expect to meet revenue goals for the second fiscal quarter of 2020, and Apple CEO Tim Cook has also said worldwide iPhone supply would be "temporarily constrained." But it wasn't clear at the time that the effects of the coronavirus would hit existing products like replacement iPhones, too

If your iPhone is heavily damaged — to the point of needing to be replaced — there will reportedly be a limited supply of replacement devices to swap it out for over the course of the next two to four weeks. The report also notes that some Apple Store locations are short on individual parts, meaning that in those cases, minor repairs that are normally handled in-store may not be possible due to shortages. This doesn't mean you're without any options if your iPhone isn't working. Bloomberg says a memo from Apple told employees that stores are authorized to mail replacement iPhones to customers whenever they become available, or loan out iPhones until a replacement arrives.

Bloomberg notes that Apple has reopened most of the China-based Apple Stores that have closed due to the COVID-19 virus. That could be a sign that other parts of Apple's business may soon function normally. Also, that Apple expects the shortage to last for up to four weeks could mean it's already ramping up the restocking of replacement phones in the meantime.

Source: theverge.com

## FUN FACT!





talk nerdy to me.

**When Snapchat first launched in 2011, it was named Picaboo**



## CONTACT US

	Fort Wayne	Warsaw
	260.440.7377	574.306.4288
	Columbia City	Indianapolis
	260.213.4266	317.426.8180



[www.preferreditgroup.com](http://www.preferreditgroup.com)



6333 Constitution Drive  
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.

