REALTOR®Mag

The Aftermath of a Tech Attack

Real estate pros who've lost money to scammers say their sense of security has been harder to rebuild.

MARCH 2018 | BY G.M. FILISKO

For years, Kevin Vandenboss didn't visit his own company's website very often. Why would he? He already knew what was on it.

Today, the broker at Vandenboss Commercial in Lansing, Mich., checks the site regularly, just to be sure it hasn't been attacked for a second time. The first time, last March, anybody who visited vandenboss.com was redirected to a porn site and assaulted with not-safe-for-work popups.

"It was some nasty, nasty stuff," recalls Vandenboss. "There were a lot of different popups ads for male enhancement and websites to subscribe to."

Kevin Vandenboss didn't realize his company website redirected to a porn site.

Vandenboss was stunned he'd become a target. "Who's going to go after my website? I'm just a local, small real estate brokerage," he explains. "Now I know. Everybody is a target."

Absolutely right, says Shawn Jaryno, a broker and salesperson at Weichert, REALTORS®, in Bayonne, N.J., who has 20 years of IT experience and teaches cybersecurity at the nearby Branford Hall Career Institute.

"Real estate is like the wild, wild west," asserts Jaryno. "Most agents are independent contractors, and everybody has their own personal email. They may be using services like Yahoo email, which has been compromised time and time again. And then people don't change their passwords."

Brokers can also be careless about the risk to their company and agents. "I've walked into offices where computers are sitting wide open [unattended] with people logged in or where I've seen a username and password right on the computer," explains Jaryno. "Agents also bring their own laptops to the office, and brokers don't know what type of antivirus software those agents have—if any—or if the software is up-to-date. I've also seen offices that have open wireless networks, and that's a problem. There are a lot of things that open this industry up to a lot of potential risk."

Vandenboss and others who've learned those lessons the hard way say the damage they suffered wasn't merely financial. Without exception, these practitioners say the most painful aspect was the devastation to their peace of mind.

Feeling Helpless

Brokers and agents who aren't attuned to basic online security in their transactions may also be less vigilant when it comes to their own data. Vandenboss has long used DocuSign to secure contracts. "But when it came to my own information," he admits, "I was like, whatever."

The trouble started right after Vandenboss had sent by U.S. mail a 1,000-piece, $1-per-piece postcard campaign that directed recipients to his website that, unbeknownst to him, had been compromised. He got an email from Google stating it had detected hacked content on his website. Vandenboss pulled up his website, which he discovered was hammered by porn and popups.

"I panicked," he says. "I had no idea what to do."

He could have contacted a "breach consultant," whose pricing varies depending on the nature of the violation. For instance, specialty insurance companies like Victor O. Schinnerer & Company—a REALTOR Benefits® Program partner for errors and omissions insurance—offer help navigating the legal and technical issues triggered by an attack.

Instead, Vandenboss dug in himself, first calling his website host, GoDaddy. He learned he had two choices: Either wipe out his website and all the files associated with it or buy a third-party program to scan and remove the site for malware. He chose the second option, which costs about $200 annually. "The scan took a couple of hours—a very, very long couple of hours," he states. "I thought I was out of the woods."

Not even close. About three weeks later, Vandenboss got a call from someone who said that while trying to find Vandenboss' phone number through a quick Google search, he was pummeled with porn again at the company's website.

This time, Vandenboss hired a tech consultant to investigate the coding at his website. Another $200 later, Vandenboss learned code deeply embedded in his site was still redirecting visitors to porn—but only when they clicked on his website in Google search results, not when they typed the website's URL into their browser.

"I ended up going all out at that point," he explains. "To log into the administrative back end of my website, I set up Google two-factor authentication. That had no cost, but I also signed up for a service called Cloudflare at $20 a month." It provides a firewall and blocks suspicious activity on his website. If it detects a suspicious internet address, Cloudflare requires the user to type in a Captcha verification word.

"I also got an SSL certificate for my site, which is usually necessary only for credit card transactions," adds Vandenboss. "But I didn't want there to be any risk to anybody filling out my contact form. That costs another $100 a year."

Still, Vandenboss couldn't shake his anxiety. "Over the next several months, every couple of weeks, I'd get an alert that my scanner found something malicious," he recalls. "It started to drive me crazy. I called GoDaddy again and was told there were probably some residual things on the website causing openings for malware."

The solution was to wipe out the entire website. Vandenboss hired another consultant—for another $200—to remove and then reinstall every file he'd used to build his WordPress website.

Today, one of the programs Vandenboss bought does a regular scan for malware at his website. "I also used to have the same simple password for everything," he says. "Now every website I use has a unique password that's long and very complicated."

In addition to the out-of-pocket costs, Vandenboss has spent countless hours recovering from the attack. He also has no idea how much potential business he might have lost after his marketing postcard apparently led people to a porn site.

The worst damage was caused by the stress. "It was the amount of time I worried about it and the anxiety it caused," says Vandenboss. "I felt the most helpless when the Google searches were still redirecting people to porn. I'd already done the things I was supposed to do to fix it, so then what was I supposed to do?"

Vandenboss now knows first-hand how vulnerable brokers are to cyberattack. "It's not somebody just sitting in their mom's basement looking for credit card numbers to steal," he states. "It's automated. Programs are crawling the web looking for vulnerabilities. It doesn't matter who you are if there's a way to get into your site. Nobody is too small to attack."

Email Hijacking

Four times Sue Dietz has been targeted, and she's sure it'll happen again.

"It's not that I'm hacked," says the agent at RE/Max Advantage in Dubuque, Iowa. "It's that my identity as a REALTOR® has been taken. They haven't been in my computer. They're sending out emails from bogus email addresses saying I have a referral in the area, and they're asking the other agent if they'd be interested in taking the referral."

Sue Dietz's identity was stolen.

The emails, which started in January 2016, are sent out under Dietz's name. The danger isn't to Dietz; it's to recipients who click on a link in the email, which likely leads to a virus or malware.

Dietz first got notice of the stunt when her office and cell phones started blowing up with calls from other agents either giving her a heads up about the scam or wondering why she included a bad phone number or link in her email. "Some are really looking for a referral and think I messed up on the phone number," she says. "Some are saying they can't open the link and I tell them that's a good thing."

There's not much Dietz can do other than to warn others to be careful when receiving an email under her name, which she's done each time it's happened and in various ways. She contacted the National Association of REALTORS®' Director of Digital Engagement Nobu Hata for help spreading the word. She also posted on her website a notice of the scam and the fact that she's aware of it.

That's not just to prevent the scammers from being successful; it's also to cut down on the time Dietz spends handling the scam each time it hits.

"Calling it a hassle is putting it mildly," she reports, since she feels obligated to respond to every call, text, and email. She's done that every time the scam starts, which has been at the beginning of each year and then again each September or October. Dietz estimates she's had 6,000 to 7,000 people contact her over the past two years. "The only way to stop this is to change offices and change my full legal name," she says. "That's not going to happen."

The scam hasn't cost Dietz money or business, except in lost time. But she knows she can't be too careful. Even though her computer wasn't hacked, she's changed all her online passwords and doesn't save any passwords in her computer.

When people contact her, Dietz encourages them to beef up their security. "I tell them that if their computer tells them to not open something, don't open it," she explains. Also, taking advice from Hata, she report the emails as spam because it might slow the scammers down. "I also suggest they let their local board know to spread the word, because usually I get hit in one area at a time," she adds.

Like Vandenboss, Dietz has been rattled by the scam. Though no one stole her computer or got into her bank account, she says, "I feel like they've taken part of my sanity away."

Phone Hostage

In the summer of 2016, an agent (who asked not to be identified) with Carolina One Real Estate Services in Charleston, S.C., checked online for a service that could help her with connectivity problems between her printer and her desktop. She found a place called WeFix, one of many sites using that name, and the business used a screen sharing program to access her computer and adjust the settings.

Problem solved, or so it seemed. She was once again able to print from her desktop.

Then on a Friday, almost a year later in June 2017, the agent, an 18-year veteran in residential sales, received a phone call from a man claiming to be with that same online repair service. He said they'd found a glitch in the work they'd done on her computer and needed to remove a program.

The caller knew exactly the amount she had paid for the repairs. He also knew they'd worked on two other devices the agent had gotten repaired at the time (she'd also arranged for repairs to her husband's and her brother's computers).

Learn how her brokerage approaches dealing with email scams here.

It'll just take a quick screen share, they'll refund her money, and she'll be set, he promised. The agent was hesitant, and she asked some questions. But she got reasonable answers to every one. So she agreed to the screen share both on her laptop and her desktop. She watched as the caller tinkered around in both computers.

Then the caller said he needed access to her bank account to process the refund. The agent grew more uneasy. She asked why he couldn't issue a credit. She even said no. But the guy was persistent and convincing, telling her this was the only way to process the refund. "Something kept on telling me, 'Don't do this,' " states the agent. "But I opened up my bank account online."

And then she realized her mistake. "I said, 'Oh, my God! You're holding me hostage with my accounts,' and he said, 'Yep, you're right,' " she recalls. "My heart just dropped."

Thus began a five-hour phone nightmare with the caller threatening harm to the agent and her family as well as the theft of all of her money. He warned the agent not to do anything "stupid" because he was watching her on her computer's camera.

The assailant kept the agent on the line and instructed her to drive to the bank to withdraw $3,000. Then he told her to drive to Walmart and purchase three $1,000 gift cards. Then he told her to go home, scratch off the coating hiding the redemption code on each card, and read each code to him.

Hours into her ordeal, the agent's brother happened to drop by, and she slipped him a note: "I'm being held hostage on my computer. Call the police." Her husband got home about the same time, and the men immediately called the police.

By then, the agent had had enough. "He said, 'I want you to get back in your car and go to the next closest Walmart,' " she explains.

She said no. The thief hurled more threats. But through tears, she held firm. "It was psychological," she says. "It was so scary."

But the agent wouldn't budge, and she hung up and unplugged her computer. The thief repeatedly called back with more threats. "He was going crazy, yelling, 'What did you do with my cards?' " the agent recalls. "He said he was going to send somebody to our house and that he was going to kill us."

Luckily, the agent and her family are safe, and her accounts were untouched. Her husband and brother raced to Walmart, where they were able to cancel the cards before the thief redeemed them. She immediately called the emergency number at each of her banks and locked down her personal and business accounts.

The next morning, she alerted the head of information technology services at her brokerage, Les Sease, about the scam. She also reported it to the Federal Trade Commission and the Federal Bureau of Investigation. She's heard nothing so far from either federal agency or from the local police about whether the online repair business was in on the scam or was hacked itself. As for the lack of closure with the case, she says, "it's frustrating, but on the other hand, I don't know of any way they could actually track down these people. This kind of thing happens to people every day, and what makes me so special?"

The agent bought a new computer and paid a tech expert—recommended by Sease—to remove the hard drive in her old computer and smash it. “I felt so violated after he’d been in that computer that I didn’t want to work on it anymore,” says the agent, who estimates she spent $1,000 on the new equipment and the tech help. “It also took a lot of time, effort, and hassle.”

Though she initially shared her story only with Sease and a few close friends, the agent now wants others to recognize this can happen to smart, successful agents. “I’m sure people think that nothing like that could happen to them,” she says. “But it was scary. It takes control of you, and you just freeze.”

The incident has changed the way the agent does business. “I’m more cautious talking with people on the phone and with meeting people places,” she says. “I’m afraid to talk to anybody on the phone if I don’t know who they are, because my trust level is very low. It’s made me very paranoid.”

Her advice to others dealing with technology issues: “If you’re having a problem with your equipment, call a reputable IT person. Don’t go through the internet. We’re so used to online everything, but face-to-face is the best.

“I’ve always known that as an agent, you should never meet anybody you don’t know at a property,” the agent warns. “This has made me even more aware. I’ve had agents tell me that they’ve met someone at a property and felt like something wasn’t right. I have that feeling all the time with all aspects of my life now. It’s sad that you can’t trust people.”

About the Author »

G.M. Filisko
freelance writer

G.M. Filisko is a Chicago area freelance and former editor for REALTOR® Magazine.