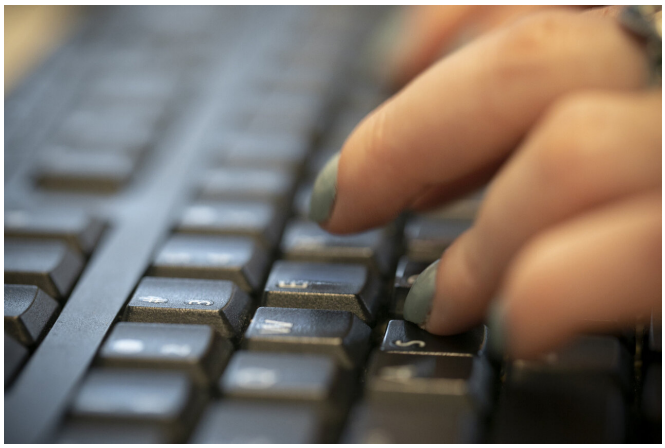
Holidays bring phishing scam surge aimed at small business

4 December 2019, by Joyce M. Rosenberg



In this Oct. 8, 2019, file photo a woman types on a keyboard in New York. Phishing scams that infect a computer and potentially allow hackers to invade bank and other accounts are highly preventable, but it takes eternal vigilance on the part of computer users. (AP Photo/Jenny Kane, File)

The email looked legitimate, so Danielle Radin clicked on the link it contained, expecting to have her products included in a holiday gift guide.

"I instantly regretted it," says Radin, owner of Mantra Magnets, a website that sells wellness products. "It took me to some random website that looked like those pop-ups telling you that you've won the lottery."

Within days of that click three weeks ago, Radin began getting notifications that people in Ecuador, China and elsewhere were trying to access her email account. She wasn't surprised; she knew her San Diego-based small business had been the target of a phishing scam.

While cybercriminals strike at any time of the year, they're particularly active during the holiday and income tax filing seasons when computer users expect to see more emails—and scammers are increasingly targeting individual small businesses with phishing scams, sending messages that look legitimate but do harm instead. An unsuspecting owner or employee clicks on a link or attachment and like Radin finds that malicious software has invaded their PCs.

Cybersecurity experts find that criminals who used to blanket thousands of computer users in hopes of fooling a handful have refined their methods. Scammers find small businesses through websites, social media sites and by combing email address books. They also mine personal data from breaches at retailers and other large companies. Then, using a process called social engineering, they construct emails that increasingly look realistic, as if they truly come from a boss, colleague, friend, potential client or vendor, a bank and even the IRS.

"In the last year or two they've been running more professional campaigns," says Perry Toone, owner of Thexyz, an email service provider based in Toronto. "It can take a couple of minutes for me to determine that they're phishing scams. That tells me they're doing a very good job."

Radin believes the scammers found her through her website or a blog. Like many small businesses, she has an email address on her site, and the scammers figured out that she might be interested in selling via a holiday gift guide. But finding a target is one thing; the scam won't work unless it tricks an email recipient into clicking. Even those who are tech savvy can sometimes let their guard down. Radin was duped even though she's the author of "Everyone's Been Hacked," a book sold online.

Often a scam succeeds because there's just a shred of doubt in a computer user—the email is realistic enough that an owner or employee feels they need to read it. Sometimes a staffer clicks out

of fear or a sense of responsibility, says Rahul Telang, a professor of information systems at Carnegie Mellon University's Heinz College.

"It might not sound very personal, but you have an idea that you should go ahead—you feel like the email is coming from the boss," he says.

In this undated photo provided by Danielle Radin, Radin poses for a photo. While cybercriminals strike at any time of the year, they're particularly active during the holiday and income tax filing seasons when computer users expect to see more emails, and scammers are increasingly targeting individual small businesses with phishing scams, sending messages that look legitimate but do harm instead. An unsuspecting owner or employee clicks on a link or attachment and like Radin finds that malicious software has invaded their PCs. (Danielle Radin via AP)

Computer users may not be looking as closely as they should at an email—there can be subtle signs that a message is trouble. Terry Cole, owner of Cole Informatics, a company whose work includes cybersecurity, recalls getting an email that truly seemed to be from a colleague. He was one of several people in the industry to receive it.

"It said that this colleague had sent me a secure private message that was ready for me to read and included a link to click. This was absolutely consistent with my normal experiences communicating with him," says Cole, whose company is located in Parsons, Tennessee.

Cole didn't do in that instance what he usually does and advises everyone to do: check the email address to be sure it's completely correct. When he clicked on the link, it took him to a bogus website claiming to be connected with Microsoft and asking him for his ID and password. He went no further and suffered no damage to his PC.

The holidays provide scammers with extra opportunities: emailed greeting cards, package shipment notices, offers of discounts—all of them false. Cybercriminals also seek personal information from owners and employees under the guise of needing them to create a W-2 or 1099 tax form; at this time of year, business owners' thoughts are turning to taxes.

"Something that claims to know you, your name, where you work and wants you to take some action is harder to spot," says Sherrod DeGrippo, senior director of threat research and detection at Proofpoint, a cybersecurity company based in Sunnyvale, California.

A common scam at holiday time is an email purportedly from the boss telling a staffer to go buy gift cards and email the numbers back, DeGrippo says.

"When it appears to come from a boss or CEO, I think there is that tendency among employees to follow those directions. They're playing on their emotions," she says.

Often, a scam succeeds in getting an employee to click on a personal email while on a company PC—many workers check their personal email while at work. Even though the email came through on a personal message, it's the company's machine that can be infected.

Companies can protect themselves in part by restricting employees' access to personal email sites, Telang says. He also suggests seminars to help staffers understand the risks that even legitimate-looking emails can present.

Some of the scams aim at monitoring a user's keystrokes. So anyone accessing a company or personal account of any sort can be giving a criminal access to their money or sensitive personal data. One tool to prevent a bank account from being emptied or a credit card maxed out is to have accounts with multifactor authentication; that requires a password and a separate code sent to a different device and that is different for each login.