Virus

from 1A

Medeiros explained how an individual or business can get ransomware on their computer:

"I get an email from Amazon that says my order was cancelled, so please click this link," she said. "I order from Amazon every day, so if I didn't know any better, I would click that link."

But by clicking that link, the user allows the virus to enter their system.

"Ransomware is completely activated by the user," Medeiros explained. "It's not something you get by just surfing online. You either clicked on something, downloaded something or opened something that executed the ransomware."

Medeiros suggests that users should always contact a company directly if they have a question regarding an online order.

"Always go directly to the source, and call the company directly,' she said. "If I get an email from PayPal, it may be a legitimate thing, but things have gotten so bad with ransomware that I'm not going to click on anything. It's 100 percent foolproof just to call the company."

Wilson is unaware how his store downloaded the virus.

"I didn't even know all this went on for a day or two," he said. "But by the time I found out about it, I think all of that was said and done and they weren't giving our files back. It was a bad deal."

Not knowing that ransomware has infected a computer is a key component to the virus, Medeiros explained.

"Usually people won't notice that they're infected until they get a warning," she said. "It's meant to be undetected because it happens over time. It's not that you click on it and, all of a sudden, your computer is locked. It starts to encrypt all of your files and slowly locks you out all of your stuff. So, today you might be able to access everything, but a week later you have no files you can get into. It's meant to be a silent killer."

Traditional virus protection programs, like McAfee or Norton Virus protection, generally don't fight against malware, according to Medeiros.

"Many people think that if they have an antivirus program, that they're covered," she said. "Unfortunately, it does not work that way. Ransomware is meant to be undetected. If you have a firewall or a virus protection program, it's not going to help."

While she did state that programs like Malwarebytes can help, they do not provide 100 percent protection. And if the virus gets past a computer's defenses, the victim is left with two choices: Pay the amount asked for or lose everything. Often, the ransom note will provide a phone number for the victim to call.

"It's hard to track the hacker down," Medeiros said. "They've gotten so good at cleaning their tracks, even when they ask you to call a phone number. Hackers can have five different phone numbers on their phone and soon as somebody calls it an activates it, they cancel the phone number, and no one can trace it."

When the hackers do ask for money, they often ask victims to pay in the online currency bitcoin.

"It's usually through bitcoin because it's not a known government currency," Medeiros said. "It's not traceable or regulated by the government. If I pay you $500 in bitcoin, there's no way to trace it. Obviously, if you sent them a credit card, they could trace the account."

Wilson stated that he would have happily paid the ransom if he felt he had done it in time, as $500 seemed a small pittance to recover thousands of dollars worth of invoices. But Medeiros highly suggested against this.

"Never pay the hackers, because once you pay it, they'll start blackmailing you every week or two, asking for more money and threatening to lock your files over and over again," she said.

But Wilson was at a loss as to what action to take.

"What do you do when it happens, call the internet cops?" Wilson asked. "I didn't seem to have a lot of options."

"Start with local law enforcement," Florence Police Commander John Pitcher said. "If you're here in Florence, call us. Then we can at least get it into a direction which can help if we can't do it ourselves. We have some abilities here. Some of that is from thousands of miles away and we have to get help from federal authorities, but at least we can get help from the right direction."

Wilson didn't call the police, not knowing that it was an option. So instead, he simply took the loss of the data and attempted to rebuild. The problem was, he didn't backup his data before the virus infected his computer.

"That was our own stupidity," Wilson said. "If we would have backed it up more religiously, that would have helped us. But I think we went a couple of weeks before we backed it up."

And without the backups, he didn't know what was owed.

"We were backtracking, trying to figure out who owed what and who we owed," he said. "It got to be quite an involved deal trying to research all that stuff and seeing from past records what was owed to us. I don't think we ever got that figured out, really. That left us with a pretty big chunk of income that wasn't available. As time went by, all of that kind of snowballed and we ended up owing the bank a lot of money. ... It ended up where we couldn't pay the paint company everything we owed them."

Backing up information is critical, Medeiros said, and can best be accomplished by storing information in an online cloud.

"There are a lot of good companies out there like Carbonite server backup solutions which will actually back up your data to the cloud," she said. "Say in January they did a full backup to the cloud, but come Feb. 1 you were hit with a ransom virus and all your stuff is locked. The good thing with having your backup is that you can revert back to the date where you weren't hit with the virus."

However, Medeiros said that users cannot just download their data back to their computer because the ransom virus is still within the system.

"You have to completely wipe the computer securely and make sure everything was scrubbed off of it, and then restore your stuff from off the cloud," she said. "That is the only sure proof way in having your files safe somewhere."

Services like these are not free, with charges varying on the amount of data that needs to be stored. Choosing to spend money on cloud protection can be a big purchase for a struggling business.

"What's your data worth to you?" Medeiros asked. "If you can't be in business because all your stuff is locked, and you can't run your company — 43 percent of businesses who have a critical data loss don't reopen their doors. They have to start from scratch."

There are other ways to backup information. Instead of using programs that only save data directly on a computer, people can use cloud-based programs like Google Docs to write and organize essential documents for a minimum monthly fee.

If the cloud is not an option, people can back up their information to an external hard drive.

"But the thing is, how do you know you're not backing up the virus? If I got hit with a virus today, and I didn't know it, it overwrites my last backup. There's no way to protect you from backing up the ransom virus as well," Medeiros said.

Wilson has since worked to implement many of these measures, continually backing up his computer and buying the latest cloud-based version of QuickBooks, which stores all of his information securely online.

"Hopefully that will protect us from it happening again," Wilson said. "As time goes by, the bad guys get smarter and they'll find ways around that. I think everybody is in that boat. You try and get the best stuff you can to protect your computer and pray that they don't find a way around it."

As for the financial future of Ron's Paint, Wilson is still optimistic. He's currently working with his paint supplier to work out a payment plan for past bills.

"I don't think we're going to be closing," Wilson said. "I'm hoping one way or another we're going to stay here and stay open. We've been here for 20 years, and we want to continue that run."

Ultimately, the best way for companies like Ron's Paint and individuals to protect themselves from such financial hardships is to be careful about what is downloaded and to make a reliable cloud backup of important files.

"Having a backup is your safest best, and education on what not to do," Medeiros said.

To help financially support Ron's Paint, a fundraiser has been set up with Banner Bank, and a GoFundMe has been set up as well, which can be found on the business's Facebook page.