Social engineering drives cybercrime against businesses

September 4 2019, by Joyce M. Rosenberg

In this Aug. 27, 2019 photo, Tyler Olson poses in his office at the University of St. Thomas - Minneapolis campus. Olson is just starting a cybersecurity company. (AP Photo/Jim Mone)

The cybercriminal who steals information or money from a small business is probably a master of deception and manipulation as well as a techno-expert.

When Nancy Butler got a call from someone claiming to be from her information technology service two years ago, she assumed it was a routine checkup by a legitimate staffer. So, as she had done many times during such calls, Butler asked the caller to confirm her account number and other information so "I could be sure they were who they said they were."

"After everything was confirmed I let them into the computer only to find that they immediately locked me out of my computer, accessed and stole from a bank account, credit card and several online accounts," says Butler, a business coach and motivational speaker based in Waterford, Connecticut. The thieves also demanded payment before they'd let her back into her computer—she didn't pay, and she found an information technology company that could unlock it.

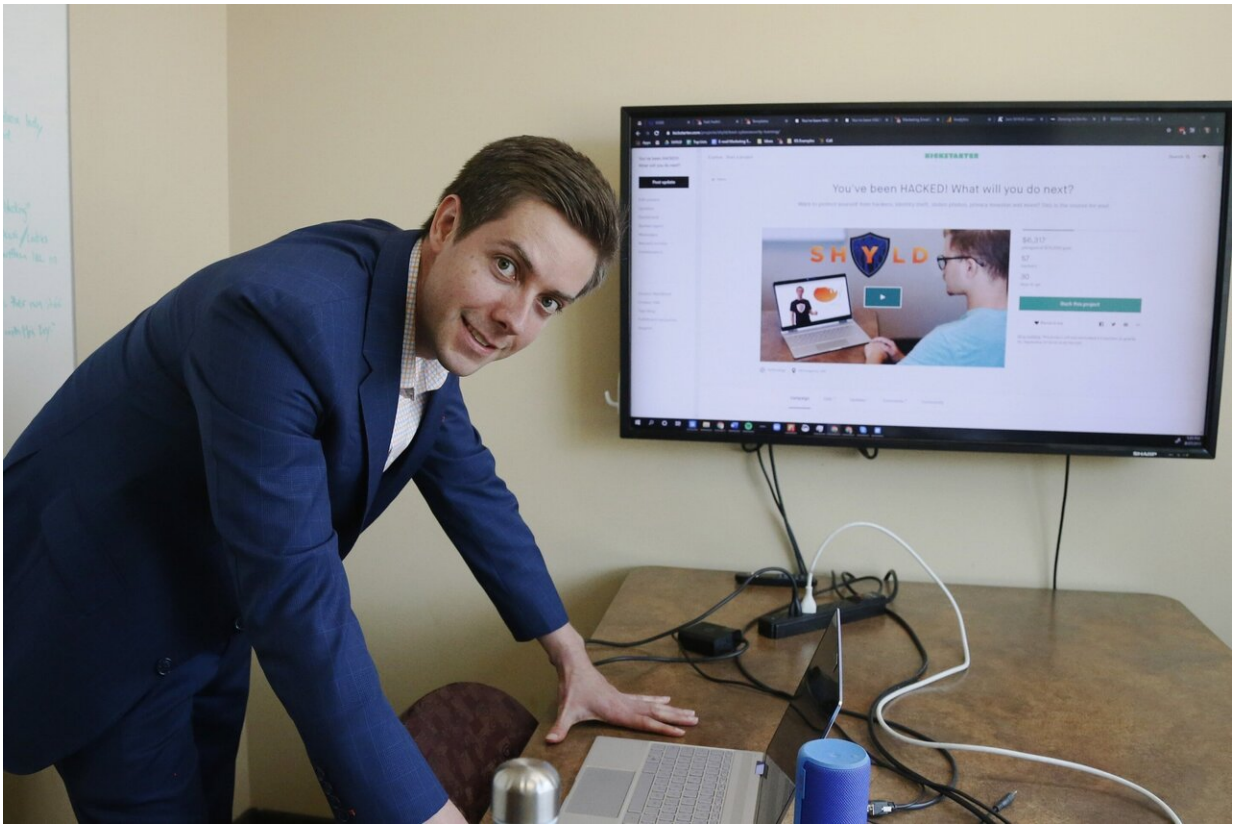
As cybercriminals step up their attacks on businesses as well as individual computer users, they're relying more on social engineering, the practice of deceiving or manipulating someone, often with email but also with phone calls, to get personal or financial information. When a business is attacked, customer and vendor data is at risk. Cybersecurity experts say small companies are increasingly being targeted.

Phishing scams often use social engineering. The scams are usually disguised in realistic-looking emails that encourage the recipient to click on a link or attachment; that click downloads malicious software known as malware that can capture information and send it back to the criminal. The emails can look like they come from a company's bank or another business. Phishing is also a way for ransomware, malicious software that locks up computers, to be planted on a device. While some cybercriminals target small businesses, malware can also be planted when an employee clicks on a personal email on a company machine.

When it comes to hacking into websites, cybercriminals still look for

vulnerabilities that they can exploit, but it's their ability to scam companies that causes many of the problems, says Terry Kasdan, owner of atCommunications, a website development company based in Northbrook, Illinois.

The kind of experience Butler had is becoming more commonplace with website attacks.



In this Aug. 27, 2019 photo, Tyler Olson poses in hits office at the University of St. Thomas Minneapolis campus. Olson is just starting a cybersecurity company. (AP Photo/Jim Mone)

"A hacker can call a business, say something to the effect of, 'I work for

your web host,' and add the real host's name to give the call credibility," Kasdan says. Hackers can get information about a website and its hosting company from online directories; then, if they're able to manipulate an employee into giving up a password, they can enter the site, steal information and damage or disable it.

A company can become a victim indirectly—its own systems don't need to be attacked for a cyberthief to steal information or money.

Tjernlund Products emailed a reorder with one of its suppliers in China and got an email back saying the company had a new bank that Tjernlund Products should make its payments to. This wasn't an unusual situation; the company's vendors in China often change banks, said Andrew Tjernlund, marketing director for the White Bear Lake, Minnesota-based maker of the maker of components for ventilating systems.

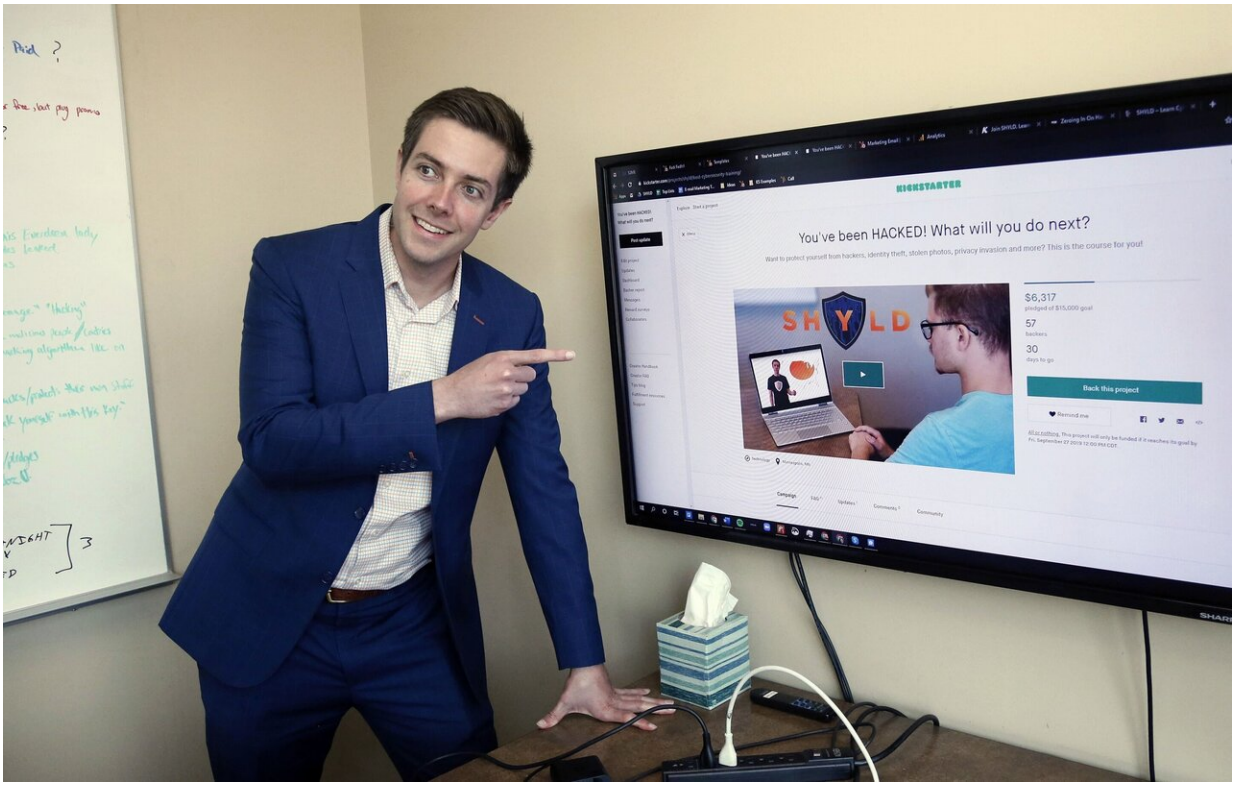
Months later, after the shipment never arrived, Tjernlund Products contacted the supplier, who investigated and found that its email had been hacked. Tjernlund Products was out about $20,000, although its supplier gave the company a sizeable break on its next order to compensate for some of the loss.

Andrew Tjernlund says he and his fellow managers realized they were indirect victims of a hacking, and that they were too trusting that the bank change was legitimate. They're more wary now.

"We test our suppliers when they change banks, ask them about what color hair we have or when we last met in person—things like that," Tjernlund says.

The government and some private companies like insurers keep count of the number of reported cyberattacks including those that use social

engineering, but many companies don't tell authorities when they've been attacked. Business owners don't want to publicize the fact that their systems or websites have been hacked; they worry about losing customers and being shunned by vendors who fear their systems could also be compromised. Cybercriminals are able to hack into one company's system through another's—when discount retailer Target had a data breach in 2013 hackers first invaded the system of a Target supplier.



In this Aug. 27, 2019 photo, Tyler Olson poses in hits office at the University of St. Thomas - Minneapolis campus. Olson is just starting a cybersecurity company. (AP Photo/Jim Mone)

The more employees and devices a company has, the more vulnerable it is, says Tyler Olson, owner of Shyld, a cybersecurity startup based in Minneapolis.

"There's an unlimited offensive capability and defense is really hard," Olson says. "It takes only one entry point in the organization."

The entry point could be the employee who clicks on an email. "Once they're inside the network, they can potentially find additional vulnerabilities. They can sit and wait or they can do some destruction immediately," Olson says

Olson, who also owns an information technology company, got the inspiration for his cybersecurity firm from his experience working on the technology team for the 2008 re-election campaign of then-Sen. Norm Coleman (R-Minn.). A video posted on YouTube showed how to hack into the campaign database; a hacker did that and the personal and credit card information of thousands of contributors to Coleman's campaign were posted on the internet, with Wikileaks claiming responsibility for disseminating the data.