OUCH! April 2023

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for You

Scareware: A Story

Warning! Your computer is infected with Black Basta ransomware. Call this phone number right away to fix your computer! - *If you saw this warning pop-up on your computer, would you call the phone number?*

The Attack

After thirty years of working hard, Deborah had saved enough money to retire with her husband. Wanting to review her retirement accounts, she typed in the name of her bank into her browser. What she did not realize is she had mistyped the bank name, taking her to a different website that immediately displayed a scary warning banner that claimed her computer was infected and instructed her to call tech support immediately. The pop-up warning was very professional. It detailed which malware infected her computer, had an official company logo, and provided an emergency number for her to call.

Deborah immediately called the number, which was answered by a seemingly professional support agent. The agent explained that her computer was indeed infected and that they needed access to her computer to fix it. She had to visit a specific website, download their security software, and then install it. She did as requested, and the support agent informed her they had access, after which they started searching her computer.

Soon they confirmed her worst fears, not only was her computer infected, but it appeared her bank account had been broken into. Fortunately, the tech support company had a direct connection with her bank, and they quickly transferred her to a fraud agent. The fraud agent confirmed her account was indeed compromised and was being used to transfer fraudulent funds. They told her to immediately transfer all of her money into a different bank account to protect it. Deborah did as instructed. They then informed her that her retirement account was also compromised. Fortunately, they also had a partnership with the government tax agency. She was then connected to a government agent who explained that to secure her retirement account, she needed to cash in her life savings and move it into another account before criminals were able to access all of it. She did this. It was a long and terribly emotional night, but Deborah was glad to not only have fixed her computer but saved all of her money by moving it to new, safe accounts. She went to bed exhausted.

The next morning, she logged into her new bank account to access her recently moved savings and retirement accounts, but all the money was gone. In a panic she called the tech support number she had called yesterday. There was no answer. She soon realized her entire life savings was gone. She had just given it away.

How to Avoid This Happening to You

Cyber criminals have learned that the easiest way to infect your computer or steal your money is to simply ask. Scareware is a common way they do this - by tricking you into thinking your computer is infected when it's really not. They then rush you into taking hasty actions so they can take advantage of you. This story is based on real events that happened to real people. Deborah's computer was never infected, instead she accidentally visited the wrong website. The tech support company was not a real company, but a team of cyber criminals half-way around the world. Even the bank fraud and government agents were just different members of the same cyber-criminal team. Once cyber criminals get you on the phone, they will try anything possible to make money. So how can you protect yourself?

- Being suspicious is your best defense. Any time someone is trying to rush you into taking an action, it may be an attack. The greater the sense of urgency and the more they are pressuring you, the more likely it is a scam.
- No legitimate company will ever ask you for your password. No bank is going to ask you to move your money.
- Never use contact information provided in an alert or pop-up. If you want to check the legitimacy of an alert, always use contact methods that you already know, such as phone numbers on your bank statements or credit cards or use links bookmarked in your browser.

If you do believe you or a loved one has fallen victim to a financial scam, report it to law enforcement and your bank right away. The sooner you report, the more likely you may be able to get your money back.

Resources

Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Browsers: https://www.sans.org/newsletters/ouch/browsers/
Emotional Triggers: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Phishing Attacks Are Getting Trickier: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/