Issued 10/13/18

How Hackers Can Ransom your Files for Hundreds of Dollars

Three years ago, Inna Simone logged onto her computer, expecting to see her standard Microsoft desktop. What she encountered instead was unsettling. “Windows along a narrow bar at the screen’s bottom were minimized; they blinked nonstop and the computer made a low-grade buzzing sound,” Simone tells The Post. “I thought something was very wrong. There was a message that my files had been encrypted and that I [would] have to install Tor” — the untraceable browser of choice for dark-web denizens — “if I [wanted] the files back,” Simone says. Simone was the victim of a ransomware attack: a type of cyber robbery wherein hackers lock you out of your own computer files and refuse to return them — unless you pony up hundreds or thousands of dollars. One out of 10 computer users has faced a ransomware attack, according to a survey of 20,000 people conducted by security-software maker Symantec. As instructed, Simone downloaded Tor, and then she received another message. “I had one week to pay $500 in bitcoin. After one week, it [would] become $1,000. After two weeks, the files [would] be gone for good. I keep pictures of my granddaughter on the computer and I wanted them back!” With help from her daughter in New York, Simone managed to secure the bitcoin. When she was ready to pay the fee, she clicked into the hackers’ one-way chat. (Yes, like Verizon, they have customer-service chat boxes) She reasoned with her computer captors until they agreed not to charge her the late fee and unlocked her files. Relieved, but still furious, she signed off by cursing them in her native tongue: “I hope you all die.” “It sounds worse in Russian than it does in English,” she says. Simone’s situation sounds dramatic enough to hold an episode of “Homeland” — in fact, the ransoming of Carrie Mathison’s top-secret computer files drove a plot point on the Showtime series last season. But ransomware attacks are all too common in

the real world, says Damon McCoy, an assistant professor at NYU. “Over a two-year period, we saw 20,000 people making ransomware payments for a total of $16 million,” says McCoy, who worked on a study that followed bitcoin trails to track ransomware payments. “And our numbers are conservative.” Law enforcement is often powerless to help, either because the viruses are too complex to crack or because the hackers reside in foreign countries with uncooperative governments. And it’s not just individuals who face cyber threats. Last month, the administrative systems of the Port of San Diego were hit by hackers. In 2017, Erie County Medical Center’s computers were besieged; the Buffalo-based organization spent $10 million to beef up its infrastructure rather than pay a $30,000 ransom in order to get its files unencrypted. When the computer system of Barnes Law in Tulsa, Okla., had 15 years’ worth of documents encrypted by cyber crooks, founder Ron Barnes made a sound business decision. “I was devastated, and we paid them the $750 or so that they demanded,” Barnes, who regained access to his data, tells The Post. “They made it an amount of money that I would be willing to lose if [the hackers] didn’t give us our files back.” While the $750 sum may not sound like much, it can add up fast for hackers, Barnes points out. “They can hit a million businesses and half may agree to the $750. Then they just sit back and collect.”