OPINION | THE WEEKEND INTERVIEW

An 'Old-School Hacker' Fights Cybercrime

After five years in prison, Kevin Mitnick put on a 'white hat.' Now he has advice for companies—and for you—about staying safe online.

By Randy Maniloff
Aug. 16, 2019 6:23 pm ET

ILLUSTRATION: KEN FALLIN

Las Vegas

You probably know better than to plug a USB flash drive from an unknown source into your computer. It could infect your machine with malicious code. But would you think twice about a cord? You should.

Kevin Mitnick hands me an iPhone charging cable. Like a magician, he asks me to inspect it. It looks kosher. He plugs it into a laptop. Then he picks up a different computer and commandeers the laptop, including its web camera.

Unlike a magician, he shows me how he did it. The USB end of the cable has been retrofitted with a tiny hardware implant. With a Bluetooth transmitter in his hand, he injected keystrokes into the "victim's" computer, which downloaded and installed malware from the internet.

Mr. Mitnick, 56, calls himself "the world's most famous hacker." Headlines in February 1995, when the Federal Bureau of Investigation arrested him after a two-year online manhunt, called him the "most wanted hacker." He spent nearly five years in prison—not his first stint behind bars—but now he's a "white hat," a hacker who abides by the law.

After his release in 2000, he tells me over dinner at the Trump International Hotel here, he decided to use his skills to "help people and help companies protect themselves." Two months later he was invited to testify at a Senate Governmental Affairs Committee hearing on computer security. He had to get permission from the probation office to travel to Washington.

Mr. Mitnick says he urged lawmakers to make it "a priority to help internal government agencies and the general populace understand the threat." He shrugs: "I tried to warn them back then, 19 years ago, but they didn't do anything."

Today cybersecurity—and insecurity—is in the news constantly. "The hackers are ahead, and the security people are always trying to catch up," Mr. Mitnick says. A week after we met in July, Capital One Financial Corp. announced that a cybercriminal had gained access to the personal information of 106 million credit-card customers and applicants. In a follow-up phone conversation, Mr. Mitnick called the data breach a "wake-up call to enterprises, and even small business, that you have to thoroughly take a look at the threats out there."

In another highly publicized incident this spring, the city of Baltimore was targeted by an attack that crippled government computers for weeks. There have been 22 such "ransomware" incidents against cities nationwide so far in 2019, according to the U.S. Conference of Mayors, which last month passed a resolution against paying off cybercriminals.

That's a foolish policy, in Mr. Mitnick's view. "These mayors just focus on 'It's the wrong thing to do because it supports the criminals' or 'Then crime pays.' But, as a business owner, I wouldn't give a crap whether crime pays. I just want to get my data back and my business back in operation."

He says victims should ask instead: "Is this 'fee' substantially less than trying to recover [the data] in other ways?" In Baltimore's case, the answer was yes: The ransom was 13 bitcoins, or about $76,000. The attack reportedly cost at least $18 million, between restoring its systems and lost revenue.

What about election hacking? "Anything can be compromised when your adversary has unlimited time, money, resources and patience," Mr. Mitnick says—and nation-states have all four. He worked as a subcontractor for Ecuador's government to secure the South American nation's 2013 presidential election from hackers trying to gain access to the vote-tallying through the internet. "There were definitely attackers," he says, "but they didn't get in."

Although he doesn't rule out that hackers could tamper with voting machines, he says it would be technically challenging. It could require physical proximity to the device, which entails a high risk of detection. He concludes that the easiest way to interfere in an election would be a simple approach—the one Russians allegedly used in 2016 against Hillary Clinton 's campaign chairman, John Podesta. Mr. Podesta received a "spearphishing" email, telling him Google was trying to reset his password. The hackers gained access to his Gmail account and published messages embarrassing to the campaign.

WANTED
BY U.S. MARSHALS
U.S. Department of Justice
Federal Bureau of Prisons
89950-012
MITNICK
KEVIN
Opinion: Former Hacker Kevin Mitnick on Jail Time and his Facebook Ban

Kevin Mitnick talks about his route into hacking and his time spent in solitary confinement in prison because the Government believed he "could whistle into a phone, communicate with a modem, and launch a nuclear weapon." Images: Kevin Mitnick / EPA Composite: Mark Kelly

Mr. Mitnick's road to a U.S. Marshals wanted poster began innocently enough. He was born and reared in Los Angeles. "When I was a young kid, I was fascinated with magic," he says. Tricks escalated into pranks: After teaching himself radio transmission, he commandeered a McDonald's drive-through intercom and used it to say sophomoric things to customers. His favorite, he recalls with a laugh, was frantically shouting "Hide the cocaine!" as a police car pulled up.

By the time he was in high school, Mr. Mitnick was committing more-serious offenses. "I would hack the phone company to pull pranks and do tricks on the phone to have fun with my friends and family," he recalls. That was known as "phone phreaking." A favorite trick was to alter the phone company's records to turn his friends' home phones into pay phones. When they tried to make a call, a recorded voice would tell them to deposit a dime.

In 1981 Mr. Mitnick went to jail for the first time, for entering a Pacific Telephone building to steal manuals on phone-system operations. Then 17, he spent 90 days in juvenile hall. But he says he couldn't stop hacking: "It was an obsession, an addiction." In 1989 he pleaded guilty to two federal counts for hacking into Digital Equipment Corp. to purloin source code for an operating system. He spent nearly a year in prison.

He then turned to hacking cellphone companies to learn about the internal workings of their latest products. His targets included Motorola, Nokia and NEC, and the FBI took notice. Mr. Mitnick knew it—he was illegally monitoring the feds' phone activity—and went on the run. After 26 months as a fugitive living under assumed names—including Eric Weiss, an Anglicized version of Harry Houdini 's given name—he was caught in a middle-of-the-night raid of his apartment in Raleigh, N.C. Agents escorted him out in handcuffs, a belly chain and leg irons. A grand jury handed up indictments on an assortment of wire- and computer-fraud charges, and he pleaded guilty.

Today Mr. Mitnick runs his own consulting firm. Organizations pay him to break into their systems and identify vulnerabilities that criminals could exploit. He says he's never encountered a system he couldn't infiltrate. He also speaks on computer security at dozens of conferences a year and is chief hacking officer—yes, that's his real title—of KnowBe4, a security company that describes itself as "a team of free-thinking techies."

Although he hung up his black hat and renounced crime some two decades ago, Mr. Mitnick distinguishes his offenses from those of today's hackers. Hacking for him was a "puzzle to be solved," he says. Even though he possessed credit-card information and valuable source code, "I could care less about making money. It was about the adventure and the pursuit of knowledge." He frequently uses the word "trophy" to describe the proprietary information he unlawfully obtained.

Mr. Mitnick is wistful for the days of "old-school hackers," whose "ethical code" said "you don't hack to cause damage to others or to make money." Things changed, he says, when companies started to do business over the internet. "I think it's more like criminals learned hacking tradecraft to better commit fraud and theft. I don't think hackers turned to be criminals."

Computer crime became easier, too. You "do not have to be technically astute to do it," Mr. Mitnick says. Today criminals offer what they call "ransomware as a service"—a sort of franchise model for high-tech extortion. Sellers on the dark web—anonymous sites shielded from search engines—offer the malicious code for sale or rent. The client sends phishing emails and induces victims to click a link that installs paralyzing code on their systems. The client makes a ransom demand. If the victim pays, the client shares the proceeds with the malware supplier. Coveware, a cybersecurity firm that helps companies respond to attacks, reports the average ransom demand in the first quarter of 2019 was nearly $13,000.

Ransomware perpetrators usually operate with near-impunity out of foreign countries. Thus Mr. Mitnick says, "Every company has to take control of the situation and analyze the risk and deploy 'people, processes and technology' to mitigate the chance that they are going to be infected." In case prevention fails, they also need "an incident-response plan in place to restore as quickly as possible." That includes having "proper backups, and not having those backups connected to the network."

The key to prevention is training. After employees see examples of phishing, their "critical thinking has just shot up," Mr. Mitnick says. But "training alone does not work." Resistance requires practice. He urges companies to phish their own employees. He dismisses the suggestion that this reduces employee morale—as long as managers explain in advance that the purpose is to "increase the abilities of the 'human firewall.' " An employee caught by a simulated attack is provided a training video.

Mr. Mitnick says small and medium-size businesses are the most vulnerable to ransomware attacks: "They don't have security staff. What they have is an on-call IT person, and usually they are calling that person when it's too late." Yet even companies with unlimited resources for security are still at the mercy of the weakest link in their chain—"the human element."

Employees are vulnerable to what hackers call "social engineering": "You can have the best technology in the world," Mr. Mitnick says, "but if I can call or email or somehow communicate with a target in your company, I can usually bypass all of that technology by manipulating the target."

Mr. Mitnick speaks from experience. As a teenager and a young adult, he was skilled at calling companies and convincing an unwitting "fellow employee" to provide him with all manner of passwords and other proprietary information to hack into their systems.

Today he can do that without social engineering. To demonstrate, he asks me for my email address and those of some people I know. With a few keystrokes on his laptop, he finds one of my passwords. My stomach turns. He points to someone else's password, which is "lawyer1." It's probably outdated, Mr. Mitnick says, but that doesn't mean it has no value: "If I was a threat actor, I'd try 'lawyer2,' 'lawyer3,' 'lawyer4,' 'lawyer5.' "

It's important, he says, to have websites generate lengthy random passwords, then store them in a password manager protected with a "pass phrase"—a sentence that could never be guessed—instead of simply a traditional password.

Impressed by his wizardry, I can't resist asking: Could Mr. Mitnick hack into my law school and change my C in Elder Law to the A that I deserved? He laughs: "I get requests for that all the time."

Mr. Maniloff is an attorney at White and Williams LLP in Philadelphia and an adjunct professor at Temple University's Beasley School of Law.