Hacker Mitnick has a plan to help you stay safe online (Q&A)

29 November 2014 12:00 pm GMT

Arguably the world's most famous hacker, Kevin Mitnick says even he's on attackers' hit lists. That's why he decided to make his next book a guide to practical safety for everyone on the Internet.

Kevin Mitnick, in 2012, shows off a bracelet that doubles as a handcuff lock pick. His next book, for 2015, will offer Internet security and privacy tips for all. James Martin/CNET

Even famed hacker Kevin Mitnick -- labeled a "computer terrorist" by the FBI in the '90s -- worries about getting hacked.

But he doesn't want you to. So he's now writing a book called "The Art of Invisibility" that shares his advice on how to stay safe online. It starts, he said, by making sure all your information is encrypted, or protected so only authorized people can access it.

"It's quite easy for somebody to get your credit report," Mitnick, now a security consultant, said in an interview this week. "In our world with all the surveillance, it's important to encrypt everything."

Thanks to high-profile security breaches at retailers like Target and Home Depot in the past year, and the ongoing reports of government surveillance first exposed by Edward Snowden in June 2013, people are more concerned than ever about their online security and privacy. Most Americans don't trust social media or online communication tools to send private information, including email, chat and instant messaging, a Pew Research study released earlier this month found. More than 90 percent said they have little or no control over how businesses collect and use personal information online.

Mitnick was convicted in 1999 after being labeled the most-wanted computer criminal in the United States and remains a source of controversy. Most recently, some in the security community have been upset over whether Mitnick's side business of selling zero-day exploits -- previously-unknown security flaws -- is ethical.

But even for a notorious computer hacker like Mitnick, it isn't easy avoiding the bad guys.

Mitnick received a tip at the end of October that somebody was going to try to hijack the website from which he runs his security consulting and public speaking business. He was able to avoid the attack because he's used to thinking about how the bad guys trick people into giving them information that lets them gain access to sensitive data -- a technique often called social engineering.

"It's really hard to help people become inoculated to these [social engineering] attacks," he said, which is why they're often successful.

To make it harder for the bad guys to crack your password, he offers some commonsense suggestions, such as using two-factor authentication -- which adds a second password or other credential to your account login. He also recommends using a virtual private network to make it difficult for people to eavesdrop on your Internet usage. VPNs protect your Internet traffic and communications so only authorized recipients can see what you're doing.

He also offered some techniques you probably didn't know about, like using sandboxing tools -- software that isolates programs -- to keep attackers at bay. Though some of these approaches, like buying a separate computer for online banking, might be a stretch for a normal user.

Here's an edited Q&A about what people should know in regard to staying safe online, courtesy of a reformed hacker.

Q: How easy is it for someone to steal your information?
Mitnick: [For example,] it's quite easy for somebody to get your credit report. [It] shows the first 12 numbers of your credit card number, so all the fraudster has to do is get the last four.

When you have an American Express card, they never report the real credit card number to the bureaus. They have a different account number. So if somebody steals your credit report, they won't get your American Express card. Sometimes, it's safer to use those than your MasterCard or Visa.

[Another example is] on mobile phones. The simple password on iPhone is automatically enabled. You can disable to get the complex password [option]. A simple four-digit password is easier to guess than a complex password, but people don't want to spend a lot of time unlocking their phones.

People like to make it really simple, that's why you have Touch ID [fingerprint reader] with iOS now. If you're crossing the border, and US customs asks you to unlock the phone, you can refuse to give them your code, but a court can make you unlock it with your fingerprint.

What are the biggest mistakes you see people making with their security?
Mitnick: The biggest threat goes back to what I did as a teenager, social engineering. There's always somebody in an organization who will... open a malicious link or an [email] attachment. It's really easy for the attacker to look for [how people know each other], especially with social networking, and create a reasonable pretext that most people will fall for.

What best practices are people struggling to adopt?
Mitnick: Would you spend $200 to ramp up your security? Everybody says yes. [I tell them to] go out and buy a [Google] Chromebook, and use it in guest mode. Only use it to access your financial institutions. Not email, not Google Apps. I think that works really well.

For anything sensitive, just use a separate machine.

It's much easier to buy a prepaid wireless device. Walk into Verizon, pay cash for a [mobile hotspot and phone] and you have anonymity. You never use it with your real mobile device, and you must go through the trouble of [changing] locations.

What should we be most concerned about protecting?
Mitnick: Anything that's sensitive to you personally. Most people focus on financial and identity theft. For me personally, it's who my clients are, my accounting, what our technologies are.

It could be something as simple as the photos on your iPhone to your financials. In our world with all the surveillance, it's important to encrypt everything.

Do you have to be an expert to use consumer security and privacy tools?
Mitnick: (Most people) don't actually realize what they're doing. You have to configure your devices for the level of privacy that you require in your life. It's a different level of privacy from what Edward Snowden would need versus the guy on the street.

How do we make security tools easier to use?
Mitnick: The people that are the most vulnerable don't use any kind of security process or security technology at all. Manufacturers need to integrate security into the devices they sell.

The biggest challenge in writing this book is what counter-measures do you give the public on something simple like protecting their email. A lot of people have access to it -- your employer has access, your email provider has access.