Hacking People: Why Your Biggest Vulnerability Isn't in Your IT Department

Shield yourself from your greatest hacking risk – your employees.

By Clinton Henry

Sitting in his favorite coffee shop, Chris noticed a marketing meeting in progress next to him. He knew it was a marketing meeting because the three people at the table had their laptop screens open to "Marketing Plans." When they got up to order coffee, they left not only their laptops but also two smartphones and a couple of memory sticks out in the open.

With careless employees like these, there's a strong possibility that sooner or later the organization will experience a breach. It's unlikely that anyone in the organization has guarded against this vulnerability by taking a serious look at how its employees operate.

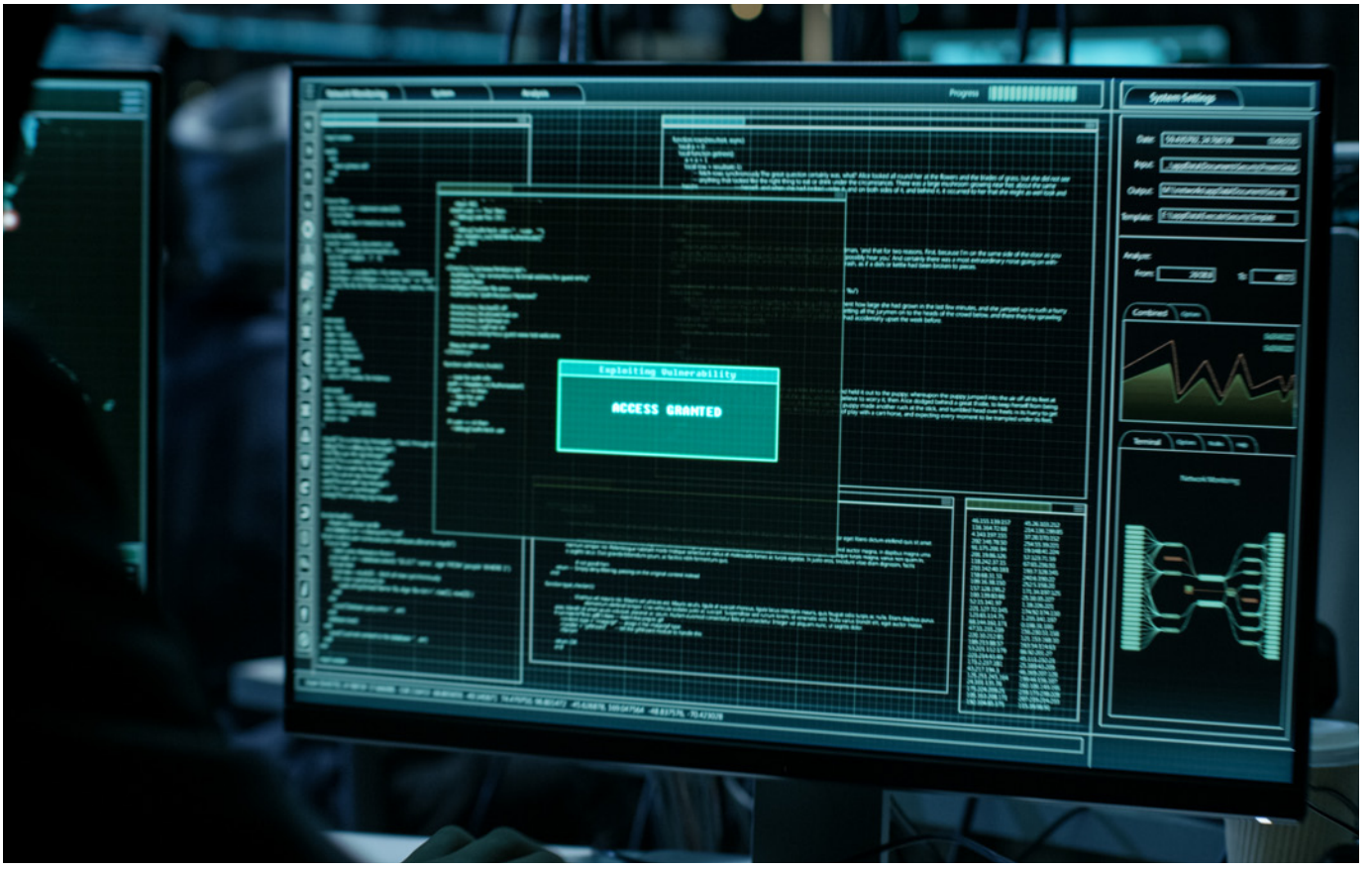
The Biggest Risk

The biggest hacking risk for any organization isn't the firewall or the server. It's another problem altogether: social engineering, which occurs when employees inadvertently (or out of malice) give cyber thieves sensitive information. The problem with most organizations is that, while they invest in cybersecurity measures, they don't invest in preventing the most common way hackers gain access: employees.

Let's review some of the socially engineered pitfalls that occur all too often:

Public Wi-Fi: Public wi-fi is to your computer network as Kryptonite is to Superman or garlic is to a vampire. It can easily be the source of your undoing. Unless you're sending out information that is encrypted via a secured site, *never* conduct *any* business from an unsecured wi-fi hotspot.

Public Places: Ever hear of "visual trespass"? It's the practice of someone in a public space looking over your shoulder to see your computer screen. It happens all the time. Sometimes the results are benign, and sometimes they're catastrophic. The employees next to Chris in the



> "Millennials are more prone to falling for phishing than older employees."

coffee shop were making it easy for any cyber thieves who happened to be nearby. In the space of two seconds, someone could have taken screen shots of the organization's marketing plan with a smartphone. A thief could easily have swiped the smartphones, stick drives, or even one of the laptops. Any document, especially any document with links to your organization, is all a cyber thief needs to get going. Never leave documents unattended.

Moreover, public conversations that should be held in private can undo an organization. In another encounter, this time in the airport, Chris overheard someone giving a coworker a password over the phone. If Chris was an opportunist, he could have started talking with the traveler later and traded business cards. Chris would then have had the man's username and organization along with his password – a perfect recipe for hacking.

Phishing: Remember those e-mails we once received from Nigeria that named us heirs to great fortunes? People fell for it in droves, handing over their credit card numbers in order to secure the millions owed to them. Then there were fake job postings that asked us for background information. The postings *looked* legitimate, and we fell for that too. Phishing hasn't gone away. It has become so sophisticated that we believe the e-mail comes from our boss, a co-worker, a supplier, or an organizational partner. The links in the e-mail are typically malware that can infect the entire network and grab important files. Don't fall for it. When in doubt, *always* verify. An interesting fact: Millennials are more prone to falling for phishing than older employees. Over-familiarity with and blind trust of technology can be a dangerous thing.

Vindictiveness: When employees leave your organization, be sure to shut them out of your network immediately. Terminated employees can be vindictive. Have a plan, and take precautions to protect your data.

Vendors: Many cyber thieves have successfully snuck in through a back door by going through vendors' networks. This is a potential problem for any organization having a continuous relationship with suppliers. If your network is "secure" but your vendors have cybersecurity that's more like Swiss cheese, it can create a huge vulnerability in your network.

> "Over-familiarity with technology can be a dangerous thing."

> "Public wi-fi is your Kryptonite."

The Best Defense

Offer your employees plenty of training. Educate them about visual trespass, phishing schemes, and other risks that can compromise your organization. Turn every worker into a vigilant protector of your organization's data. That's the best way to guard against the social engineering attacks that can lead to cyber disaster.

Clinton Henry (clintonhenry.com) is one of the world's leading cybersecurity and identity theft experts. Known for his engaging keynotes and insightful perspective on cybersecurity, Clinton has amassed a loyal following of executives who look to him for guidance on how to protect their data and reputation from attack or compromise.

Keep Your Data Safe

Ramp up your security with these articles at NonprofitWorld.org:

- **Nine Surefire Ways to Lock Down Your Cybersecurity** (Vol. 36, No. 3)
- **The Purposeful Techie: Nonprofit IT with Intention** (Vol. 30, No. 5)
- **What Is the Board's Role in Managing Risk?** (Vol. 15, No. 5)
- **Don't Get Caught by Phishing Schemes** (Vol. 35, No. 2)
- **Avoid Catastrophe by Addressing Cyber Risk** (Vol. 33, No. 3)
- **Seven Questions You Must Address to Thrive in the Digital Age** (Vol. 35, No. 1)