Auto Casualty

Three Reasons Your Data Is Under Attack Right Now

June 22, 2020
4 MIN READ

Erez Nir

When the COVID-19 pandemic hit and states began issuing stay-at-home orders in March, many organizations likely scrambled to implement secure remote-working systems and policies for their employees. Many businesses, including Mitchell, had a head start when the stay-at-home orders came, as we already had secure remote access systems in place. Many recent industry and government articles discuss essential security technology required to mitigate risk for remote work access, but focusing just on technology misses a key element of security. The best technology available today won't close the most vulnerable gap—humans.

Three Reasons Your Data Is Under Attack

The research company Gartner says they are seeing "massive uplift" in phishing and other related attacks during this time—an increase of more than 400% in the last few months—primarily targeting the human factor in our security structures. Experts have proposed many reasons for this rise in attacks, but they can be grouped together into three key factors:

1. The Emotional Nature of Our Changing World

Combine the environmental challenges of remote working with the stress and uncertainty in our world right now, and you have an ideal breeding ground for security attacks. Phishing attempts are more successful when they leverage current events, and we're in the middle of an unprecedented amount of upheaval and change. Malicious actors can tap into fear about the pandemic, concern about jobs, anxiety about family members and even positive desires to be financially responsible or support our executives to drive the desired actions from their targets. Our nature is to be helpful and trusting, but we have to temper it with caution and verification when these land in our inbox.

2. The Blending of Personal and Work Time

Many employees are working remotely long-term for the first time. This newly remote workforce has introduced a cultural security risk for organizations. When employees are working within an office setting, they think like an office worker. Everything around them—the lighting, the office décor, the murmur of productivity—reminds them that they're working, which helps keep office policies and protocols in mind. Those same visual and audible reminders aren't there while working from home, so the temptation to relax secure behaviors is greater. No one is looking over their shoulder, and the office peer pressure to follow security protocols is missing. They may have just taken the dog for a walk or helped fix lunch for their kids. Personal lives are blending with work lives, and it is unavoidable that at some point during the day they will not be in that "I'm at work" mindset. That's when they are most vulnerable to social engineering attacks, and only fresh training and reminders on how to spot and avoid those attacks will keep it top of mind.

3. Company Equipment Is Being Used for Things Other Than Work

Training your employees to be safe and focused during work hours can make a difference, but they need to be reminded that security issues can just as easily happen outside of work hours. Unauthorized programs can conflict with work applications, and online software tools and games can expose a computer and the company network to malware or other malicious tools. Company devices should be reserved only for company work. Employees should also never let family members use work devices, even for seemingly benign activities. No one wants to have to explain that it was their child's browsing activity that triggered unsafe website warnings.

Have You Recently Trained Your Remote Workers?

Leaders responsible for information technology are more intimately familiar with security risks and dangers than employees, so we often overlook how important it is to remind employees frequently of how to keep company data access secure. Just because an email was sent or instructions were given in an all-hands meeting two months ago doesn't mean your employees shouldn't be reminded again of their role in protecting both company data and their own personal information. We can't control what's happening in the world around us, but we can control how effectively we train our employees to help protect them and our organizations. The number one thing we can do is communicate often with our remote workers. Stay connected with them, and offer different types of reminders and training to teach them how to spot and avoid attacks. By varying what you share, you increase the chances of your messages sticking. For example, at Mitchell, we conduct tests where we send our own "phishing" emails to employees to see if they spot and report the attempt as well as ongoing communication and education programs that run throughout the year. So far our training is working, and focusing not only on security technology and tools, but also the human aspect, has helped to safeguard our business and the information of our customers. Fortunately, there are many educational resources available. There are also several free resources that can help and could be ideal for additional training. While all tools and practices should be vetted by your internal security and legal teams, here are just a few to consider:

- FTC—Cybersecurity for Small Businesses
- Director of National Intelligence—Know the Risk Raise Your Shield
- National Cybersecurity Alliance—Staying Safe Online
- Wizer Security Awareness Training Videos
- Google's Online Phishing Quiz

Stay safe, and stay secure!

enlyte

mitchell | genex | coventry