HR Insights

Brought to you by TechServe Alliance

Preventing Cyberattacks on Remote Employees

The COVID-19 pandemic has solidified remote work as a new operational standard. Employers should expect this trend to only grow in the future. In fact, many major companies, such as Twitter and Microsoft, have indicated that remote work will be an indefinite option for their employees.

While this is exciting in many ways, remote work also comes with unique challenges—namely, cybersecurity. This article discusses some cybersecurity risks that remote employees face and offers potential solutions.

Cyber Threats to Monitor

Hackers have been assaulting businesses since the first computer was invented, always trying new methods of gaining critical information. Depending on the size of the organization, it may receive dozens or thousands of hacking attempts each day. These attempts are typically brushed aside by IT security teams and firewalls. However, with employees working from home, those protections aren't as guaranteed.

The following are some of the most common cyber threats facing individuals:

- **Phishing and vishing:** Phishing is an attempt to gain personal information, such as computer passwords, Social Security numbers or other data. Hackers and scammers will impersonate a legitimate company and send fake emails to solicit this information, typically with a phony threat. Vishing, or voice phishing, takes this process a step further. This is when a scammer spoofs a legitimate phone number (from within the organization or otherwise) and poses as an IT help desk, using that alias to solicit personal information. These calls may even be routed to personal cellphones, making it harder for organizations to catch. Vishing attempts are a recent trend, but are increasingly prevalent. Employers should review existing cybersecurity policies to directly address vishing.

- **Malware**: Malware is a type of computer virus that is typically disguised as an innocuous program, email attachment or link. These viruses infect computers and can do any number of tasks, typically hidden to the user. For instance, they might store password data, track website activity or download personal files.

- **Brute force attacks**: Brute force attacks are when hackers try logging into someone's account many, many times. These attempts work most often when individuals reuse usernames and passwords across different accounts. A hacker may expose the information to one account, then use those credentials everywhere else they can think of, eventually gaining access.

These cyber threats are made worse when employees are working from home, especially if they

conduct business on personal devices or don't connect to a secure network. That's why it's important for employers to proactively address cyber threats with their remote employees.

Protecting Remote Employees

There is no single solution to avoiding cybersecurity threats. But there are key steps organizations can take to protect their employees and critical data. Below are some of them.

- **Behavioral analytics tracking software**: This is software that monitors each individual's computer habits. Since hackers can impersonate an employee, it's hard to detect when someone's credentials have been compromised. With analytics tracking software, the program would be able to spot when a user is displaying abnormal computer usage. This will depend on the individual, but it may include accessing certain files or transferring large chunks of data.

- **Automated threat detection software**: This software is like antivirus programs found on many computers by default. It can scan files and detect malicious programs automatically. Automated threat detection software often pairs with other efforts, such as behavioral analytics.

- **Comprehensive work-from-home guidelines**: Using personal devices to conduct business is an easy way to compromise usernames and passwords. Employers should set clear guidelines regarding acceptable technology to use (often a work-provided laptop) and work locations. For instance, cafes may be off-limits because they often have unsecured networks.

- **Employee education**: Education and training are perhaps the best protections against cyber threats. Employees should know basic cybersecurity tactics, such as how to spot a phishing email, how to recognize a scam caller and how to report a potential security breach. They should also be instructed to not reuse login credentials, especially between work accounts and personal accounts.

Employee education is especially important, as hackers and scammers become more sophisticated each week. Employers should keep an eye out for new scams and alert employees as needed.

As with any successful initiative, cybersecurity protocols must be observed by all stakeholders within an organization. That means educating everyone, from the top down, about how to protect themselves and their workplace from cyber threats. If even a few individuals go without proper training, the entire organization could be compromised.

As the business world becomes more connected, cyber threats will get more sophisticated and commonplace. Start educating employees about cybersecurity today to better protect your organization.