Why Businesses Need to Think Like Hackers This Year

TechRounder PDF Edition

Live article: https://www.techrounder.com/business/why-businesses-need-to-think-like-hackers-this-year/

By Vipin PG | Published February 10, 2023 | Updated January 4, 2026 | Format: Explainer | 4 min read

In brief

Cybercrimes are rising, especially after the pandemic, because people now spend more time online than ever. With that said, it is clear that cybersecurity professionals need to change their approach to fighting cybercriminals.

Cybercrimes are rising, especially after the pandemic, because people now spend more time online than ever. With that said, it is clear that cybersecurity professionals need to change their approach to fighting cybercriminals.

Businesses of all sizes should maintain the cybersecurity rules they have been implementing for years and become more proactive. Cybersecurity teams would benefit from keeping up with the latest hacking techniques and detecting network or system vulnerabilities before cybercriminals. If you want to be more active in fighting cybercrime, here's where you could start:

Protecting the IoT

The Internet of Things, or IoT, is becoming increasingly popular worldwide. The latest data from 2022 show there are 13.15 billion devices connected to IoT, which will grow in the future. IoT devices are not used only in homes, as businesses of all sizes are modernizing their offices with the latest smart gadgets.

Unfortunately, some of these devices can be exploited by cybercriminals and used to access a whole network. When a hacker gains control of IoT devices, they could mess with your office and employees, especially if you use smart locks. Luckily, you will prevent these attacks by regularly updating the firmware on your IoT devices and learning how to use a VPN.

Secure all Devices

Every device accessing your business' network should run the latest antivirus software. Ensure the employees working from home on their personal devices know this too. Both Windows and OSX computers have default antivirus software that works incredibly well.

You could also consider using a VPN, especially if most of your employees work remotely. This service encrypts the information sent or received, and cybercriminals won't be able to access it. Teach them how to use a VPN regularly and all the benefits of this service. Also, instruct your staff not to use jailbroken devices to log into your network, as they can be very unsafe.

Use a Backup

Preparing for every situation is a must, so create a backup and have it ready in case you experience a cyberattack and can't access any of your data. Switch on the automatic backup during the setup, and you won't have to think about it. You could set it up for daily backups if you have new important information coming in regularly.

You can choose the data you want to keep in your backup. However, the backup should always include customer information, documentation related to your business, log files, and configurations. These will help your company even if you are locked out of your network and experiencing ransomware.

Software Updates

Cybercriminals often find vulnerabilities in outdated software. Therefore, updating the software is a must. First, ensure manufacturers still support the devices you and your employees use to connect to the network. Running an older operating system could be risky because it doesn't have available updates.

Patches are the most important part of every software update because they are made to fix potential software vulnerabilities. Set up automatic software updates, and you won't be required to keep a close eye on the latest releases. Additionally, talk to your employees and ask them not to use unsupported devices to connect to the network. It includes smartphones and tablets too.

Train your Employees

While having a cybersecurity team is recommended for every business regardless of size, remember that all employees need to be aware of potential dangers. Invest in training your employees about cybersecurity trends, and they will be able to spot a phishing attempt in time and much more.

With the proper knowledge, your employees can deal with a security breach in real time and work together to prevent it or minimize the damage.

Learning to recognize a potential security breach and stop it at the very beginning can prevent major losses for a company. While most businesses might be thinking about cutting back on their budget, paying for cybersecurity training should be mandatory. It is the best way to ensure the data is safe.

Two-factor Authentication

Two-factor authentication can protect both your customers and your system. Anyone logging into your network must provide a code besides the username and password. It is one of the best ways of ensuring no third party has access to your system.

Securing your business through two-factor authentication ensures protection against phishing. Even if a cybercriminal manages to get their hands on login credentials, they won't be able to access your network because they still lack the authentication code. Protect every important part of your system, such as client information, documents, social media accounts, etc.

References

1. explodingtopics.com - blog / iot-stats - https://explodingtopics.com/blog/iot-stats

2. nordvpn.com - blog / how-to-use-a-vpn - https://nordvpn.com/blog/how-to-use-a-vpn/