How Business Leaders Can Teach Their Team About Cybersecurity

Image Source: Pixabay

In today’s digital landscape, we are confronted with an overabundance of cybersecurity dangers. As a small business owner, this reality can be incredibly daunting, especially considering the financial impact that data breaches can cause. However, equally as important as knowing the cyber dangers present outside the organization is knowing how your team can learn to protect themselves and, by extension, the company from malicious attackers.

In this article, we’ll be discussing how business leaders can take progressive steps to prepare themselves for today’s cybersecurity threats and how they can teach their team to prepare for the worst.

Create a Cybersecurity Training Schedule

With cyberattacks targeting more small businesses than ever before, employee training becomes increasingly important for every business owner to reduce organization attack surfaces and limit the chance of getting ransomware or other dangerous malware. One way to do this is by prioritizing a cybersecurity training schedule for all employees.

To do this, business owners can begin by creating an internal cybersecurity team that includes members from various departments within the business. This group should meet regularly to discuss ways to improve messaging around each person's role regarding data security and what they need to do if their working device is compromised or stolen. Cybersecurity training then becomes everyone's responsibility instead of just one department's problem to solve alone.

When training, it's essential to start with the basics. Employees should be taught what a phishing email looks like and how to avoid clicking on links that could lead them to malware-infected websites. Training sessions should be conducted frequently so each person can refresh their memory as needed. Businesses might even consider running training simultaneously every month or year, so people don't forget about this information over time.

Incorporate Internet Safety Into Company Culture

Business leaders can teach their team about cybersecurity by training employees on what to look for when encountering suspicious behavior online. Employees should be trained in cyber security best practices and recognizing phishing attempts, malware warnings, unsolicited emails asking for passwords or confidential information (usually paired with an urgent tone), etc. If any of these signs are present at work, employees should report them immediately so IT professionals can investigate the issue further. Having robust internet safety training is vital because most data breaches occur due to human error – not technological complications.

By embedding internet safety into company culture, small business owners can better prepare their employees for cyberattacks and data breaches while ensuring that new employees adopt the same urgency. This is especially the case if you have employees who are working from home. You must encourage them to adopt smart home practices, such as stronger internet connections, to both save energy and save data.

Practice Safe Data Management

As data breaches become more common, small business owners need to take steps toward ensuring that their employees are practicing safe data management procedures. It may be tempting to believe that your business doesn't have anything of value for cybercriminals to steal; however, even if customers or clients do not regularly share data with your company over the internet, you still hold a significant amount of sensitive information in paper form, which can easily be compromised by an individual who has access to your office space overnight.

Every staff member must understand how serious cyberattacks are, especially when harming both individuals and the businesses they work for. To protect customer data, it may be helpful for small businesses owners to utilize an offline digital data storage device, such as a flash drive or portable hard drive, which can hold all of the information collected by your employees with limited risk of exposing sensitive data online. This would allow you to keep records on hand while still taking appropriate precautions against cybercriminals who constantly find new ways to infiltrate even the most secure systems.

Implement User Access Control

Another way for business owners to limit the digital attack surface of their employees is by implementing user access control systems and solutions. User access control restricts user activity based on what user is assigned to which types of tasks. For example, a user who works in accounting will have read-only access to the financial applications they need for their work. At the same time, an IT developer tasked with writing code should only be able to write and edit code when using company servers or networks.

User access controls also monitor user behavior, so business owners can identify if someone is trying something malicious without being detected by specific security solutions such as firewalls and endpoint protection software. Additionally, this type of user monitoring ensures that all actions taken in a network are traceable back to its source, whether it’s from internal sources or external ones. This makes it easy for businesses to see how data leaves their organization over public internet connections.

In Conclusion

Internet security is becoming more and more important, with data breaches occurring all the time. By putting these precautions in place, small business owners will better prepare their employees for cyberattacks and data breaches while ensuring that recruits adopt the right level of urgency towards cyber safety.

Author Bio:
Adrian Johansen is a writer and consultant in the Pacific Northwest. She loves sharing knowledge with others and learning along the way! You can find more of her writing at **Medium**