6 Tips to Stop Hackers from Stealing Your Data and Your Business



Only you and your employees can ensure your organization’s future security.

March 20, 2018 4 min read

Opinions expressed by *Entrepreneur* contributors are their own.

You’ve started your own company. As the chaos subsides and systems begin to take shape, you
ask yourself – have I been hacked?

The answer is simple: Count on it.

If not already, then you’ll be hacked soon – within the first year after you’ve opened shop. Regardless of a company’s size,

getting hacked is an unavoidable fact of life. Smaller companies are the most vulnerable. So, how can you defend yourself?

Assume you've already been hacked — and go on high alert. When you assume you've been hacked, it forces everyone to take action: To see risks in everything you do, in every tool you use, in every product you develop, and every vendor you choose. That's the world we live in today. It's not just an issue for security or IT, but for
everyone in the organization.

Related: Crime-as-a-Service Could Be the Next Big Threat to Your Business

Here are six tips to instill the right "I've-been- hacked" mindset in your company.

1. Avoid blinders.

Your IT team may be experienced, sophisticated and trusted, but they're still human. As such, they'll develop blind spots or get stuck in narrow thinking. Engaging outside consultants to validate your security approach objectively will help keep the blinders off, while adding third-party KPIs to measure your success.

2. Implement Privacy by Design.

Privacy by Design (which calls for privacy to be taken into account from beginning to end of the engineering process) is a best practice approach to protecting customer data when developing applications. Be sure it's a priority for any software vendors you use. Privacy by Design isn't new, but It's more important today than ever.

Related: 3 Biggest Cybersecurity Threats Facing Small Businesses Right Now

3. Build a strong information governance program.

Even the smallest companies need a solid information governance program. Among the benefits: Understanding where your valuable data is, who has access to it, and what information you can delete to reduce your attack surface. You should also make sure your core systems come from trusted, world-class vendors.

4. Field the right team.

Fighting cybercrime is about more than hiring people with computer science degrees. It’s about attitude and disdain for complacency. Look for inquisitive people who are hungry to learn and interact well with others. It’s important as well to have a Chief Information Security Officer (CISO) with the ability and authority to lead.

Related: The Worst Data Breaches in the U.S., Ranked State by State

5. Empower through education.

Continual education at every level of the organization is key, and not just with an annual hour-long e-training session. Think regular executive updates, an employee hub, workshops, videos, contests – whatever it takes to keep people focused on security. Training in data analytics and machine learning is especially valuable, as they’re the future of cybersecurity.

6. Take a pledge.

At McAfee, we believe so strongly in security that our employees take a pledge. It’s part education and part ensuring that all employees take personal ownership of the security

mission. If making security personal works for security experts, consider how it can up-level the game in your company, too.

I'd like to be able to guarantee that taking all these actions will keep you safe. But you don't want my guarantee – what you want, and need, is to realize that only you and your people can ensure your organization's future security. What I'll guarantee is this: When company leaders act like they've been hacked, they're better prepared and better able to survive the increasingly inevitable threat.

https://www.entrepreneur.com/article/310697