

5 Steps to Take If You Get Hacked



When you get hacked, do you know what to do next? Getting hacked is not a matter of if, it's a matter of when. Chances are, you will get breached. The moments that follow are critical to reducing the harm from the attack and keeping your company alive. This checklist will walk you through the exact steps to take when you're breached. Use it to make sure your staff doesn't make a bad situation worse.

1

Respond

If you suspect a breach or other cybersecurity incident, immediately disconnect all affected systems from the internet. Report your suspicions to your cyber incident response team or managed IT provider. NEVER power off your system.

2

Mitigate and contain

Keep affected machines off internet access until they can be verified as clean. During that time, supervisors and managers must determine how employees can stay productive without putting the company at further risk.

3

Report

This incident needs to be reported to your insurance company as soon as possible. Executives and company ownership must prepare a public statement to ensure full transparency with customers and stakeholders.

4

Recovery

Your recovery plan should be in line with your business priorities. All machines must be verified as safe before they can be reactivated or restored and used again. This should be done by a cybersecurity professional to ensure they are safe to use.

5

Prepare

Cybersecurity should never be taken for granted. If you've been breached once, you will likely be targeted again. However, even if you've never had an incident, don't wait to prepare until it's too late. Create an incident response plan that's tailored to your business. Then, run a tabletop exercise to test your plan and work out any issues so it flows seamlessly during a real event.

A Managed IT Provider Can Help Increase Confidence in Your Cybersecurity

1

Plan Ahead

We get it – most businesses are worried about cybersecurity but don't understand it. Planning ahead dramatically improves your ability to survive a cybersecurity attack.



2

Train Your Staff

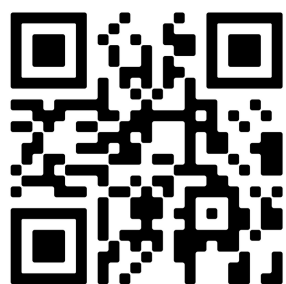
Cybercrime is a billion-dollar industry because they target busy workers. Phishing emails and ransomware traps are not anywhere near as obvious as they once were. Training your staff is the best way to avoid getting breached in the first place.



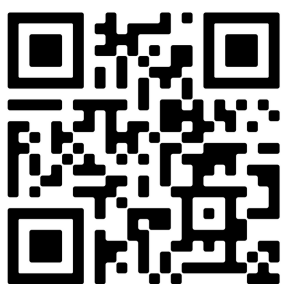
3

Work With Us

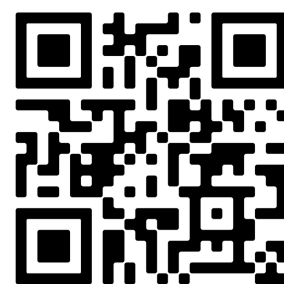
You shouldn't have to be a cybersecurity expert just to keep your business running and profitable. Cybersecurity is increasingly complex and essential for all businesses. DiamondIT is a security-first managed IT services company. We manage all your IT safely so you don't have to worry about it ever again.



Get The Guide



Train Your Staff



Book A Consultation

877-716-TECH (8324)
www.diamondit.pro