HISCOX
SMALL BUSINESS INSURANCE

Helping small businesses defend their digital data

Here's a list of things you can do to help keep your data safe from hackers, and what you need to know if a threat actor infiltrates your system.

CHECKLIST

Prevention

- [ ] **Use strong passwords**

  Password managers like Last Pass can generate a random password when you first set up an account on a new site. It will be stored in the password manager so you don't have to remember it, and it will be much harder to crack because it won't be your dog's name or your anniversary.

- [ ] **Change your passwords frequently**

  If a password of yours is compromised you may not realize it right away, and once you do it may be too late. So get in front of it by changing your passwords every 90 days.

- [ ] **Use multi-factor authentication**

  Which requires you to enter a password and then verify your identity by entering a code you receive on a different device. To add multi-factor authentication to an existing account, check the security settings on the account, and look for 'multi-factor authentication' or 'two-factor authentication.'

- [ ] **Keep your software up to date**

  Whenever a program or operating system asks you if you want to update, the answer is 'yes,' and the sooner the better. You can also run patch management software on a regular basis will help ensure you don't miss any updates.

- [ ] **Make sure your Wi-Fi network is secure**

  Make sure your Wi-Fi network is encrypted with WPA2 (WiFi Protected Access 2) or WPA3 and that your password is secure. WPA3 is more secure than WPA2 so if your network supports WPA3, use it.

- [ ] **Control physical access to devices**

  Only authorized staff should have access to your company's devices, and only to the ones they need.

- [ ] **Back up your data regularly**

  Either to the cloud or to an external device that is stored away from your physical office space.

- [ ] **Monitor your system for unusual activity**

  Using an intrusion detection system or security information and detection management system. These systems will monitor your network and detect any unusual activity.

- [ ] **Educate yourself and your employees**

  On how to recognize a phishing email or smishing message, and how to recognize and report a suspected cyber incident.

- [ ] **Have a security plan in place and keep it up to date**

  Develop a written plan for what to do in the event of a cyber attack, including whom to contact and what to do immediately. Revisit the plan at least yearly to be sure it's current.

↗ For more information visit:
hiscox.com/SBDC

Detect

☐ **Monitor your network**

An intrusion into your network will leave evidence, so regularly monitoring your network can alert you early to unusual activity that could indicate a breach has taken place.

- Install a monitoring tool
- Establish a baseline
- Review logs
- Set up alerts
- Assess your vulnerability
- Monitor external connections
- Run your monitoring tools regularly so that you know what your network looks like when it's healthy.

☐ **Watch your bank account**

Cyber criminals will sometimes process a small transaction to verify that the account is open, before they go in for a bigger amount.

Mitigate

If you find that, despite your best efforts, your network has been compromised, you want to contain the damage as best you can. Time is of the essence, so do these things right away:

☐ Implement your response plan

☐ Contact your cyber security insurance company

☐ Remove the compromised device from your network if possible

☐ Contact your IT staff or consultant, or a breach response consultant.

Should you pay a ransom demand?

One of a business owner's worst nightmares is getting a ransom demand from a hacker. You'll likely be told that your system has been compromised and your data will be inaccessible until you pay a ransom, often in cryptocurrency. Ransom demands are often in the millions of dollars, even for small companies.

There's a lot of debate around whether a cyber ransom should be paid, and for good reason. First of all, your data is already in the hands of a threat actor, who may be using it for nefarious purposes even before you know it is gone. Plus, there's no honor among thieves. These are criminals, after all, and just because they are saying they will restore your data after you pay the ransom doesn't mean they will. In fact, The 2023 Hiscox Cyber Readiness Report found that half of those who paid a ransom were shaken down for more money than the original demand, and half also didn't get their data back even after paying up.

The most critical tool for mitigation is cyber security insurance. In addition to protecting your business from the costs associated with a data breach, hack, or other cyber incident, insurance provides you with expert breach response resources that will minimize the cost, inconvenience, and potential damage to your reputation. **To learn more about cyber security insurance, and find out how much it will cost for your business, visit Hiscox.com.**

22291 8/24