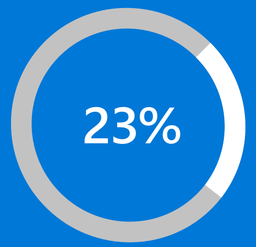

Microsoft
How to fight back if you've been hacked

Introduction

Cybersecurity incidents have become more and more common for small and medium-sized businesses, making it critical to know how to prepare and respond. If your business hasn't been hacked yet, it could very well be next. A study by the Better Business Bureau found that 23% of small businesses (≤ 250 employees) reported having been the target of a cyberattack, with nearly half of those occurring in the preceding 12 months.[1] Read on to learn about the four stages of an attack and what you can do protect, detect and respond to reduce your risk and repair the damage.



23% of small businesses have experienced a cyberattack[1]

01.

A foot in the door

Hackers use any vulnerability they can to gain network access. Some of the more common methods are:

- **Exploit.** Taking advantage of software vulnerabilities, particularly out-of-date software, to access information or install malware.
- **Malware.** Malicious software that can steal information, send spam or lock your systems.
- **Ransomware.** Malware that locks users out until a ransom demand is met.
- **Password spraying.** 'Spraying' common passwords at multiple accounts at once to gain entry.
- **Phishing.** Malicious links in legitimate-looking emails that trick users into giving information..
- **Watering holes.** Malicious links placed on websites frequently visited by a target.

All that sounds bad, but you can fight back. Start by assessing your first line of defence: your user credentials and accounts. Some planning and prevention now can make it harder for hackers to breach your systems later.

Examine your level of **control** over user access. For example, can you revoke access if an identity has been compromised?.

Look at the who, what, why, where and when of your **network access**, and follow up on anything that seems unusual.

Employ **multi-factor authentication** that requires users to provide additional verification beyond just a username and password to confirm their identities.

Protect **user credentials** and control access using solutions designed to guard against identity breaches

Have all employees use **strong, unique passwords** or consider taking a password-free approach by using facial recognition, fingerprints or PINs for secure sign-ins.

02.

Setting up shop

Once an intruder is in, they look for ways to gain more control by identifying and impersonating accounts that have management privileges, which gives them deeper access to your systems. Hackers use a variety of methods at this stage, including:

- **Keyloggers.** Malware that records each key a user presses to collect usernames and passwords.
- **Network scanning.** Exploring and cataloguing a target list of accessible network resources
- **Pass the hash (PtH).** Using a victim's underlying identifying code (hash) to authenticate access remotely, without the need for the actual user credentials.

How do you fight back?

Conduct a **risk assessment** to understand the assets you have, the potential risks to those assets, the cost to your business if those assets are leaked and the controls you have in place.

Create an **incident response plan** to make sure you are ready in the event you detect a breach

Select **appropriate security solutions** based on your assessment. Look for solutions with features that detect malicious activity in your system, provide key insights about where and why the attack happened, and enable a fast response to stop the attack and mitigate the damage

Bring in professionals to help if you don't have enough dedicated IT resources. A service provider who specialises in security issues can be your best ally.

03.

Expanding their territory

Once an attacker has widespread access to your network, they will infiltrate as many systems as possible. They may look to establish means for long-term access while evading detection using malware 'implants' installed without your knowledge. Some common techniques hackers use are:

- **Botnets.** Networks of computers infected with malware and controlled by a hacker to launch co-ordinated, large-scale attacks.
- **Command and control (C&C).** Servers and infrastructure used to control multiple computers through centralised commands, such as a botnet.
- **Living off the land.** Exploiting your systems using your own network resources (as opposed to malware) while maintaining a low profile

Fight this stage at the data level:

Understand where your data resides, whether it's on a server, personal phones or computers, in the cloud or some combination.

Monitor data regularly, keeping track of who is accessing and sharing information and revoke access to documents, data and apps as necessary.

Classify data by sensitivity, then focus on the most sensitive and critical information with defensive efforts such as encryption and access restrictions.

Back up critical data, preferably in the cloud, and have a system in place to do so regularly.

04.

Making themselves at home

Some hackers just want to get in, get something and get out – in other words, a smash-and-grab approach. But others decide to stay a while. Longer-term hacking techniques include:

- **Advanced persistent threats (APT).** These are hackers who stay on the network long-term, continuously stealing information while remaining undetected.
- **Backdoor.** An entry point that allows an attacker to come and go as they please for as long as they want.

The last thing you need is a scattershot approach, leading to an ineffective response against an increasingly sophisticated attack. Fight back by integrating your solutions through a comprehensive security strategy.

Work on gaining a **comprehensive view across all of your assets** to understand your company's risks and ongoing security situation.

Develop consistent **security policies** that balance productivity and security.

Manage user identities, devices, apps, data and networks in a co-ordinated way for maximum protection.

Monitor and **update** your security approach continuously.

Protect, detect and respond

In the modern workplace, every business has to deal with the potential for hacks. Rather than wait for something bad to happen, prepare ahead of time. You can significantly reduce the chances of a hacker gaining access and greatly decrease harm if they do. Follow the steps outlined here and use this free security assessment tool to get more ideas. You can fight back against hackers.

[1] Better Business Bureau. '2017 State of Cybersecurity Among Small Businesses in North America.' https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf