
# HOW TO TELL IF YOU'VE BEEN HACKED

Small to medium businesses (SMBs), by their very nature, are at a disadvantage when it comes to combating cyberattacks. The fact that they are a smaller business means they likely don't have the same IT staff in place as large companies, or the large budgets required to shield them from the ever-increasing number of attacks. Simply not having the resources available, and therefore having less robust security, puts SMBs at a disadvantage to prevent and mitigate a cyberattack.

According to Untangles 2021 SMB IT Security Report, the top barriers to cybersecurity for SMBs are Employees who do not follow guidelines (28% of respondents) and budget (27% of respondents). While large corporations have the resources in place to detect a breach, smaller companies with fewer detection and security measures in place, rely on themselves and employees. Being able to recognize suspicious activity can help SMBs spot the attack and minimize damage.

**Businesses should look for the following to identify an attack:**

## 1. RANSOMWARE MESSAGES

This may be the most obvious notification that you've been hacked and unfortunately it means your data has been encrypted and risks being held hostage unless ransom demands are met. Most victims end up with many days of downtime and additional recovery steps even if they do pay the ransom.

## 2. SLOW COMPUTER OR BATTERY DRAINING QUICKLY

If the battery starts draining quickly or your computer suddenly starts crashing or running as fast as a tortoise, you may have been hacked. It could be malicious software running the background slowing down your computer and draining the battery.

## 3. SUSPICIOUS FILE CHANGES

If you notice that files have suddenly been deleted for no reason, or document or folders names randomly change, this could be the handy work of a hacker and should be investigated immediately.

## 4. ANTIVIRUS OR ANTIMALWARE PROGRAMS ARE DISABLED

Has your antivirus or other security software suddenly been turned off? That could be a sign that you've been compromised with malicious software.

## 5. PASSWORDS SUDDENLY DON'T WORK

If you're sure you've entered the correct password and it's still not working, you could be the victim of a hacker who has accessed your account and changed the password to keep you out.

## 6. UNWANTED INSTALLATIONS

Unknown browser toolbars and/or software installed on your computer are not only signs that you've been hacked but they can open malicious files and release malware, disable your antivirus, and cause more unwanted changes.

## 7. OTHER UNUSUAL ACTIVITY

- Internet searches are redirected
- Mouse pointer makes clear movement between programs and makes selections
- Attempted access during odd hours or from odd locations
- Frequent and random popups

**SMBs already are at a cybersecurity disadvantage with smaller budgets and staff. In addition to monitoring for the signs of compromise above, here are measures every company can take to protect themselves:**

- Train employees continuously. As security adversaries find new ways to infiltrate networks, keeping employees trained and up to date will only strengthen your network security.
- Use multi-factor authentication to provide an additional layer of protection of sensitive data.
- Backup your data. If your data is backed up, even if your network is breached, a backup can revert the machine to the data it had on it the day before the attack, minimizing losses.
- Segregate your network for different types of usage and roles. For example, have a guest network that is separate to the main network.
- Keep software up to date and install all software patches expediently to avoid a breach.

# ABOUT UNTANGLE

Untangle enables organizations to address network concerns and remain vigilant against unauthorized network access. The Untangle Network Security Framework provides IT teams with the ability to ensure protection, monitoring and control for all devices, applications, and events, enforcing a consistent security posture across the entire digital attack surface.

# UNTANGLE NETWORK SECURITY FRAMEWORK

## *ADVANCED SECURITY*

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

## *INTELLIGENT SD-WAN*

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Untangle AI-based Precitive Routing technology for first packet, dynamic path selection
- Manage one or many appliances from Command Center

## *CLOUD MANAGEMENT AT SCALE*

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints