www.AdviseITSolutions.com
(951) 777-2004

I Think We've Been Hacked!

A business guide on what to do when you think your network has been breached.

Ever get the feeling that things just aren't right with your computer or your network? Things may be running slow, you may be getting weird pop-ups, your passwords aren't working as they should be, settings have gone a bit wonky, or you no longer have access to all your files. Chances are you have been hacked.

Discovering the breach is half the battle – but what are you supposed to do next?

STEP 1: Alert your IT company.

The sooner you tell your IT company, the quicker they can protect the rest of your company's network, either by isolating your system, utilizing tools in their arsenal to minimize damage, or restore your data from a pre-breach backup.

STEP 2: Change all passwords.

Update them to something completely new, not just a password that you utilize in other systems, you never know how much data this hacker has stolen.

STEP 3: Use two-factor authentication.

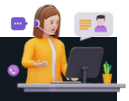
This extra step can stop hackers in their tracks even if they have your current password because you have to input information from two sources: (password+phone or password+email) to gain access.

STEP 4: Watch other accounts closely for ongoing impact.

It's possible that the hacker only gained access to one account, but if they gain access to one, they likelycan quickly gainaccess to other accounts.

STEP 5: De-authorize connected apps.

De-authorize any apps that you may have connected between accounts. Your goal in a breach is to isolate yourself as much as possible to reduce the impact of collateral damage.



STEP 6: Monitor your financial accounts and information.

Pay particular attention to your financial data. Consider adding a flag to your account for major transactions until your IT company gives you the all-clear.

STEP 7: Alert appropriate colleagues/clients.

If you suspect the hacker has access to your email, customer data, or social media, inform your colleagues and appropriate clients about what's going on.

STEP 8: Run a virus/ malware scan.

Your IT company has likely already done this for you, but if you don't have a managed service provider, run a robust virus/malware scan on your own to diagnose what you're dealing with.

STEP 9: Figure out where your sensitive data has gone.

Once your data is out there in the world, there is no real way to get it back. We recommend utilizing a Dark Web scanner to quickly identify potential breaches and weak points.

STEP 10: Plan staff / individual training.

Quarterly all-staff training, as well as individual training for any individuals who seem to be struggling, is recommended. If someone repeatedly falls for a phishing attack, they undergo extensive training.

Realizing you've been hacked is one of the most painful, violating experiences you can have with technology. Today, it's happening more often than ever before. Utilize this guide to know what to do next if you suspect a hack, and be sure to contact us to answer questions or to get your team going on your new security plan.

Contact Us to Get a Free Consult