Oh "!*&^" Our Website Just Got Hacked!

Posted At : November 29, 2017 12:17 PM | Posted By : Admin
Related Categories: Your Business, Security

About once a month, we get the call - "Something or someone has hacked our website, email, desktop, or server." The calls rarely come from regular Computing Center clients but it does happen. We are there to help and have a lot of experience in recovering and restoring and getting systems going again. This article from HP descrbes the major steps that are taken to deal with hacks. You can do-it-yourself, but as we tell our clients - we do this work all the time and isn't your time better spend doing what you do?

What do you need to do to get your site back online? Three steps to recovery.

After the initial panic subsides, your mind starts racing and you find yourself asking the question, “What do I (or my IT folks), need to do to get our site back online?” Read on for more...

What are the first few things you do when the alarm goes off on Monday morning? If you're anything like me, your morning ritual includes a bold coffee blend and a quick perusal of social media before settling down at your desk for the day.

Now, imagine that same scenario with a very different ending. This time, as you kick your feet up behind your desk, you notice dozens of errors cascading across the browser as your website struggles to come to life. Your site's been hacked. That nightmare inspired this website security checklist. Consider it your “next steps” guide, should such a catastrophe rudely interrupt your morning routine.

Step one: Name that hack

Step one is all about deciphering what type of attack brought your site to its knees. A bit of a no-brainer, but important to the list nevertheless. We'll cover three of the most common attacks here.

- **Ransomware**: This one's the easiest to recognize, because that email sitting in your inbox demanding large sums of money is a dead giveaway. Gaining popularity, ransomware attacks can hide your website's data behind advanced encryption methods until you pony up the dough.
- **Phishing**: These attacks operate on the premise “there's a sucker born every minute.” When that tempting email or phone call finds the right person, hackers can siphon all the authorization info they need. Once you've been fleeced, hackers can hijack your site and even use it in future campaigns. Phishing can be spotted by connecting the dots between a gullible user and your newly remodeled site.
- **Denial of Service**: If your site can't be found when the address is typed in a browser, there's a good chance DoS or DDoS is to blame. When countless automated calls for your page or another service on the same server flood its connections, your website will choke.

Step two: Quarantine without prejudice

You know your site's been hacked, and you've got a good idea how it happened. The next step is to apply some IT-related first aid to stop the bleeding.

The quickest way is to shut down the compromised server. While you may have a hunch as to what took your site down, you probably won't know the extent of intent for some time. As such, it's better to be safe than sorry, and make sure the attack doesn't spread like Kerrigan's Zerg empire.

While this may seem like a logical first step, it's surprisingly difficult to quarantine effectively if you don't

first know what's attacking. Pulling up your disaster recovery site is pretty useless if a phishing attack stole your credentials. Likewise, throwing another site up immediately following a DDoS attack is only adding more fuel to the fire.

It's better to be overzealous when quarantining rather than keeping sites live and spreading the disease.

Step three: Exterminate and restore

You've revealed the attack and had Scotty take the affected systems offline—now what? It's time to destroy the threat. This step will look slightly different depending on the attack discovered in step one.

Should you happen upon a phishing attack, quarantined systems will need to be scanned and scrubbed for any malware. You can use the Symantec virus database for that. It'd also be a good idea to change passwords. Consider multi-factor authentication, and have a little heart-to-heart with the more gullible users in your environment.

DDoS attacks will need to be waited out or otherwise filtered and diverted. If your servers are being overwhelmed, you'd be wise to invest in some traffic flood prevention further out on the network perimeter to quell future attacks.

Ransomware will either require a hefty Swiss bank account or a considerable amount of elbow grease and luck to be rid of. Thanks to the efforts of some white-hat folks, however, full recovery is possible—as pointed out by Bleeping Computer.

Finally, we have one last suggestion: Take some time, when the fire is fully extinguished, to learn from the event. What could have been prevented? How could a resolution be more quickly achieved? What can be done to avoid a similar attack in the future? (When our technicians and engineers are doing the extinguishing, we are already looking for solutions to prevent similar events from occuring.)

While checking off these three items should get you back up and running, learning from any mistakes made will help you adapt in this unforgiving digital world.