I've been hacked! What do I do?

By John Mc Loughlin

21 Feb 2020

With all the hype around cyber attacks and every single cybersecurity enterprise talking about cyber resilience to improve a business' security posture, nobody really knows what to do once they've been hacked.

John Mc Loughlin

These terms are being used extensively and yet it still does not really help the consumer understand the importance of exactly what it means and what they can do to lower their risk.

Often the focus on corporate risks and acceptable use policies is lost on the end-user. Constantly referring only to the policy will not influence staff to adjust behaviour. In order to make real change, one needs to focus more on procedures, steps and the personal impact of better cyber hygiene to help employees be more secure.

More importantly, when employees know what to do and what to look out for, they will be better protected at home and automatically by association more secure at work.

Companies need to address the pressing aspects of cybersecurity and try to cover these issues in a way that will make sense to the non-technical user.

It is amazing how making small adjustments can positively influence the behaviour of staff and improve security at the same time. When the employee makes the changes themselves, positive results follow.

Passwords passwords passwords

Before anybody says that passwords are not the best form of security, or they are outdated and the like, the truth is that we live in an interconnected world and every single system we interact with needs a password. Every system, cloud storage, app and network that we place our information and login credentials into, increases our risk landscape.

When you use a single password for every platform, a breach of one is a breach of them all. You may practice safe cyber activity and still have your credentials compromised in a third-party app that has poor security measures.

Password policy

A password policy is not only something that you should have in the office. It is a good idea to come up with, follow and assess compliance to a policy for your personal passwords as well. This policy, at work or home, must be practical for your situation. Have a look at the systems and platforms that you work with and follow the policy to ensure password security.

If you make use of a password manager, ensure that it is secure and use it correctly. How often will you change your passwords and will you only do this when something is compromised - monthly or quarterly? Whatever the decision, this is your policy and make sure you follow it.

How will you monitor for compliance and breaches? Ensure that you keep your eyes open for breach notifications, update managers and regularly check for multiple online sessions or logins on all your platforms. Also, register for a breach notification service on your personal email accounts.

Contract a service provider to monitor and search for stolen, compromised and leaked credentials online and on the cyber underground. Breaches happen every single day and knowing that credentials have been part of a breach allows you to take the required steps to stay secure.

Implement multi-factor authentication on every platform possible. The reality is that the extra 2 or 3 seconds it takes to punch in the code or verify the login is far simpler than trying to recover data, chase lost money or explain how your credentials were used to drop ransomware on those around you.

Make sure your passwords are unique to you. With the growing number of platforms and passwords, take the steps necessary to secure yourself and always follow your policy.

ABOUT JOHN MC LOUGHLIN

John Mc Loughlin is a visionary entrepreneur that has been involved in the setup and management of a number of start-up businesses. For the past seven years, he has been working towards changing the security landscape for SMEs in South Africa through his company, J2 Software, which provides solutions around reducing risk and improving compliance. John is an industry specialist and thought leader in the security space, and his particular areas of expertise lie in planning and strategising.

- #BizTrends2023: Continued explosion of cyberattacks - 13 Jan 2023
- Many faces of malware: Are you protected? - 2 Mar 2021
- Data breaches becoming more common - 16 Oct 2020
- I've been hacked! What do I do? - 21 Feb 2020
- The complex and challenging world of cyber risks - 11 Dec 2019

View my profile and articles...