Addressing human cybersecurity risk: lessons from Pokémon Go

James Young-Drew
Solicitor

July 2016

Speed read

The recent Pokémon Go security scare is a perfect example of why employees are one of the biggest cybersecurity risks for businesses.

Millions of employees and business owners around the world downloaded the wildly successful Pokémon app within days of its launch, many with potential access to their company's data.

The Pokémon phenomenon shows how easy it is to unwittingly provide third-party access to sensitive digital information.

It also illustrates that defusing cyber threats requires more than firewalls and anti-virus software. The human element is important too. Below, we discuss why people are almost always the weakest security link in an organisation, and what businesses should be doing to manage this risk.

This article first appeared in the *National Business Review*.

The Detail

Earlier this week, millions of Apple device users of Pokémon Go were alarmed to discover that Niantic, the creators of the augmented reality app, had "full access" to their personal Google accounts without user authorisation.

It was believed that "full access" permitted Niantic to read your email, send messages on your behalf, access Google Drive documents, and more. Niantic accepted that the permitted access was wide but said that the app only accesses basic Google account information, such as user names and email addresses. The company quickly released a fix.

End of story, right? Not at all.

The problem is that Pokémon fans granted that "full access" to Niantic, and therefore access to much information, irrespective of whether Niantic voluntarily held back from pursuing these rights. What about the next provider with "full access"? Will they benevolently refrain from exploiting access conceded by users (usually without realising they've done so)?

Here's the lesson at the heart of all this: people often unwittingly provide third-party access to sensitive digital information.

Everyone wants to catch Pokémon, after all.

In addition to the personal privacy implications, the risk for businesses is significant.

Peter Bailey, GM at Aura Information Security, says the episode is about the fallibility of humans in relation to cybersecurity.

> *"People are almost always the weakest security link in an organisation. No matter how secure a company's systems are, if it doesn't have the policies, procedures and security culture in place to ensure staff fully understand the risks, it leaves its business open to attack.*
>
> *We often use social engineering in our work to highlight vulnerabilities.*

Addressing human cybersecurity risk: lessons from Pokémon Go

It can be a simple matter to get staff to click malicious links through phishing attacks, download infected files, or even trick a call centre into giving us a system password."

Businesses which use a Google Business account, or have employees downloading risky apps on devices used for business purposes, could be easily compromised in this type of situation. Not only could sensitive commercial information and IP be accessed, but this opens up another vector for a cyber-attack.

Email access can also be manipulated in more imaginative ways. "Whaling", which is a variant of a "phishing" attack, involves using an employee's hacked email account to request information or funds from within the employee's own company. These messages appear legitimate to the recipient, and can cause serious harm.

The Pokémon phenomenon highlights two further issues.

- First, some Pokémon fans may have downloaded black market apps in their haste to obtain the game. One rogue version was found to contain backdoor malware called DroidJack that takes control of a device. Malware is a major risk for employees and businesses.
- Second, the speed with which Pokémon took over many workplaces illustrates how businesses have little to no time to react to cyber threats.

As with this Poké-craze, cyber-attacks don't announce their arrival in advance. They come from left-field. Businesses must be prepared regardless.

We've written several articles about the duties of directors and executives in relation to cybersecurity, and concluded that most boards in New Zealand are in breach of their legal obligations by failing to ensure that sufficient cybersecurity counter-measures are in place.

Pokémon Go - a serious phishing hazard?

This includes addressing the human element of cybersecurity, says Mr Bailey.

"Companies must have up to date information security policies implemented in the business, as well as a recent response plan for when an attack happens (not if, but when)."

Policies around the usage of a business-issued device – especially a mobile device – should be clear, and regularly checked for compliance.

Changing company culture through a variety of exercises is also important. This includes regular staff training in security awareness, internal staff exercises such as phishing campaigns, and regular Red Team exercises, where an external security company tests your defences against a person-based attack."

Businesses should be asking themselves: if this Pokémon Go scare had turned into something more serious, would we have been ready?

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com