How many abandoned online accounts do you have?

By Riaan Badenhorst

14 Feb 2020

For some reason, our online accounts always seem to miss the proverbial 'spring' or 'New Year, new me' cleans ups. But if we are honest, there are probably a couple of them that aren't in use anymore and can in fact be closed and deleted.

Riaan Badenhorst, general manager at Kaspersky in Africa

We all tend to do it - create an account to access something, share some details to gain access for a particular reason, but then simply stop logging in – because we don't need the account anymore - but never bother to delete the account.

In fact, there must be millions of abandoned accounts – accounts that just sit there, lying dormant – yet still susceptible to being hacked. And of course, if they were to be hacked, you probably wouldn't be the wiser.

So, if you are not using a particular account anymore, does it really matter? Yes, it most certainly it does!

An abandoned account has the potential to be exploited to gain access to resources and important information about you. For instance, even outdated information about you gives criminals insights and means to exploit your personality in various ways: from illegal usage of your photos to the identity theft.

In addition, abandoned accounts might have information that could be used in attacks on other accounts you have. If, for example, your data, including passwords and logins is stored in the plain texts, the criminals could potentially use it to access other accounts with the same or similar passwords.

What's more, any personal information compromise opens possibilities for spam and phishing attacks on you or the company you represent. This is relevant not only for mass-mail out of malicious e-mails but also for carefully crafted targeted campaigns.

Don't leave your data unattended

This is why it is important to understand the risks and responsibilities of leaving your data unattended. And why a conscious effort to close those old and abandoned accounts should be part of that New Year clean up focus.

Firstly, it's important to know the difference between deactivating an account and deleting it.

Deactivating is like turning off the 'lights'. People won't see your name or photos, for the most part, and you can't use your inactive account. But you can turn those 'lights' back on automatically, simply by logging back in – where your settings, friends and messages (if social media-based) and everything else will be exactly where you left them when you come back. Deleting, on the other hand, ensures the account is closed and if you haven't saved or backed-up the data on that account or app for example, it will be lost.

Review dormant and inactive accounts

Secondly, it's important to look at the types of accounts you could have created and left dormant or inactive, and the very real risks that these accounts pose.

A few examples could include:

- **Social network accounts**: not all people regularly check all their accounts. While some profiles may actually be used to login to other services, others are forgotten about and replaced by new ones. Social networks will continue to send e-mail notifications but, they often get filtered into a separate folder that you quit checking long ago – so when there is unauthorised access you won't know.

- **Backup email address**: many people have one, a separate e-mail account for mailings and notifications so as to not clutter up your main inbox. You may use it to enter competitions and for registering everything and anything, but you don't check it very often as there are no important incoming emails. Therefore, you may not notice for a long time that your backup e-mail has been hacked - at least not until you lose access to a very important account.

- **Online store accounts**: linking a bank card to a store account makes online shopping easier, especially if you are a frequent shopper. The profile is also likely to contain your home or work address for delivery of goods, plus other valuable personal data. But of course, there comes a time when you may stop using the service. If the account remains live and bank card details are stored there, not on a separate server, cybercriminals may have access to all your data in case of compromise. In worst-case scenarios, you may find out about only when they try to buy something in your name or even worse, money comes off your account.

As you can see, even an unneeded account can cause a lot of problems if it is hacked or hijacked by dubious cybercriminals. So, make sure you revisit the online services and apps you have registered for, clear all the cache and saved information, turn on account login notifications in services that have this option and that you are likely still going to use - and review those notifications promptly. And very importantly, delete those accounts that aren't in use anymore. After all, preventing a problem is much easier than dealing with its consequences.

ABOUT RIAAN BADENHORST

Riaan Badenhorst joined Kaspersky Lab in January 2011. He headed up the corporate sales division, focused on growing Kaspersky Lab's market share in both the Enterprise and SMB sectors in sub-Saharan Africa. In October 2012 Badenhorst was appointed as managing director for the Africa region and has been heading Kaspersky Lab operations in the region ever since.

- How many abandoned online accounts do you have? - 14 Feb 2020
- #BizTrends2018: The developing cyberthreat landscape - 15 Jan 2018
- #BizTrends2017: What will the cyber threat space hold in 2017? - 10 Jan 2017

View my profile and articles...

For more, visit: https://www.bizcommunity.com