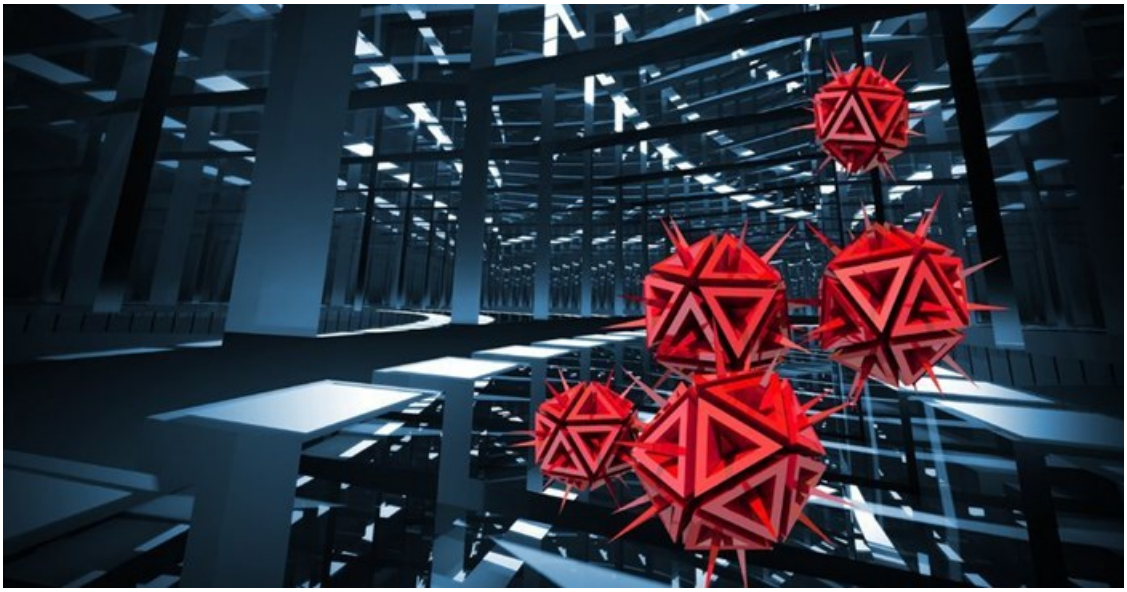
BIZCOMMUNITY

Cybercrime is everywhere because businesses aren't educating

By Simeon Tassev

11 Apr 2018

Cybercrime has overtaken all other types of crime as humans have embraced digital technology without really understanding it.



Now, as digital, mobile, and social technology becomes an integral part of our personal and work lives, the score has changed - we are beginning to comprehend its weaknesses and our vulnerability and how this unanticipated security risk extends to the enterprise.

There are the basics that everyone teaches their kids, their customers, and their employees – don't give you passwords away, set up one-time security pins and, if it's important, ensure double and triple layers of security. Encrypt.

But what about the malware and ransomware that is just one careless and well-camouflaged click away?

And the new cons everyone's being caught out by simply because, well, they don't know enough. Like the cryptocurrency scams.

Don't spend another cent on cybersecurity until real risks have been assessed

Charl Ueckermann 6 Apr 2018

While every business will have policies and controls in place on the corporate network, there is very little they can do about staff using technology in their homes and in their everyday interactions. The bugs, malware and Trojans they pick up can and do enter the enterprise.

There are simply no boundaries anymore.

The answer? Education.

Businesses have to start educating technology users, not just protect the business.

Security policies

There is no all-for-one security policy that works any longer. A security policy must be highly relevant to the organisation. The injunctions are simple:

- Understand the technology.
- Understand the risk.
- Put the right policy in place for your business.

> *There is, unfortunately, no winning formula. Nor can businesses simply put in security requirements for the sake of ticking a box anymore.*

Accepted levels of risk need to be defined and the security policy and rules must be practical and enforceable.

The security at any organisation will depend on the systems in use. Enterprises need to identify entry points to their networks and put endpoint protection in place, control access to and monitor traffic on these networks, sweeping networks clean regularly.

How to avoid falling prey to a Facebook/Cambridge Analytica-type scandal

Ilse van den Berg 26 Mar 2018

The enterprise must also ensure the security circle is closed, putting alerts in place and acting on those alerts, staying ahead of new and emerging threats and enforcing basic safeguards, such as ensuring users implement anti-malware on their phones.

> *As the extent of our digital exposure and vulnerability continues to unfold, it's clear that businesses need to take more responsibility for educating its users.*

The rights and privileges we give digital platforms and applications, like Facebook and others, are being exploited in unexpected and surprising ways. It's time we wised up – there are very few benevolent providers of free apps and functionality.

The digital world is in its infancy and there are untold and as yet unknown ways in which our data and our online behaviour can be manipulated and cashed in on.

Companies have a lot to lose — it’s time to ensure everyone takes responsibility for putting the basics in place.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa

- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...