

Bezos case exposes billionaires' vulnerability to hackers

February 10 2019, by Luc Olinga



A tabloid illegally obtained a naked photo of Amazon CEO Jeff Bezos, the world's richest man

The stunning revelation that a tabloid obtained below-the-belt selfies of Amazon founder Jeff Bezos—the world's richest man—suggests that

even billionaires are not out of the reach of hackers.

Bezos came out fighting this week, accusing the National Enquirer of blackmailing him with lurid pictures of him and his mistress, and pre-empting the threat to publish by releasing details of the images himself.

But for Mark Johnson, CEO of Sovereign Intelligence, the incident makes clear that "no one is beyond the reach of cyber exploitation."

"It's a curious irony that billionaires demonstrate astounding acumen related to their own industries, and yet seemingly ignore the minutiae of common-place security measures."

Johnson sees billionaires and top executives as especially vulnerable because their [personal information](#) is a gold mine for criminals, intelligence agencies and competitors.

"Obtaining their personal data is like having keys to the kingdom," said Johnson, potentially providing priceless insight into the thinking and strategies of the world's most powerful business leaders.

Ian Bremmer, the founder of the Eurasia Group think tank, put it more bluntly.

"If the National Enquirer has @JeffBezos dick pics, don't tell me China doesn't have @Amazon IP and strategy," he tweeted.

Increase in calls

Since the revelations about Bezos, whose fortune is estimated at more than \$130 billion, computer security experts interviewed by AFP report an increase in calls from wealthy clients asking them to verify that their computer systems and devices were not hacked.

"Today's threats however are not necessarily trying to breach the walls of the castle—they are already inside, residing on personal devices," said Kris Coleman, the founder of Red Five Security. "Experience has shown that the typical breach is not discovered for eight months."

In this ever-more connected age, more and more [personal data](#) is stored online—from [social security numbers](#) to bank details, driver's license numbers and personal addresses.

As a result the focus of security measures for the ultra-wealthy has shifted from bodyguards and sophisticated alarms towards risk management to protect their assets, their image and their "legacy."

The super-wealthy will typically have their own computer security service and also call on external companies for regular evaluation of their devices because a large number of hacks are detected by third parties, according to observers.

Mark Zuckerberg, Facebook's CEO, spent \$7.3 million on his security in 2017, up from \$4.2 million in 2015—astronomical sums that the social network deemed justified due to his prominence.

Last July, Facebook said it would give him \$10 million more per year to strengthen his security.

"Protection from colluding insiders working from positions of trust; or, against an intelligence agency trying to attack from the outside is going to require a large investment, a lot of experience, and vigilance," said Coleman.

Entourage

For Johnson, "no one's data is that well protected. Think of all the third-

party platforms that have your social [security](#) number, or banking information, or that hold your personal pictures."

Just days before Bezos disclosed that a tabloid had obtained his intimate selfies, a fellow billionaire—Joe Ricketts, the founder of the broker TD Ameritrade Holding Corporation—was ensnared in scandal following the release of private messages.

The American news site Splinter published a series of racist emails from Ricketts, without saying how it obtained them.

The exchanges, some of which date back to 2009, show the 77-year-old sharing and apparently endorsing racist jokes and conspiracy theories. He has since apologized.

Back in August 2015, a [cyber attack](#) on the Ashley-Madison extramarital dating site revealed that American billionaire Dan Loeb had an account there.

Bezos did not say how the National Enquirer obtained his pictures, but experts say the most common method is for a hacker to usurp the identity of a member of a person's entourage.

"The adversary would send a message to the target asking them to click on a link in a text or email," Coleman explained. "The sender's real identity is hidden but the target trusts the message from their 'friend' and clicks the link unlocking malware or another type of attack on that device."

© 2019 AFP

Citation: Bezos case exposes billionaires' vulnerability to hackers (2019, February 10) retrieved 9 April 2024 from

<https://phys.org/news/2019-02-bezos-case-exposes-billionaires-vulnerability.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.