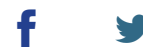# Hackers are lurking, and we must protect ourselves | Opinion

By Andrew M. Korge

SunSentinel

Hackers are lurking, and we must protect ourselves | Opinion

By **Andrew M. Korge**

SHARE THIS

Get serious about cyber security.

JANUARY 17, 2017, 12:53 PM

"Y ou say it can't happen to you, until it happens to you." These were Miami Beach Mayor Philip Levine's words after the city discovered that $3.6 million was stolen from a government bank account, possibly by a hacker.

Between this incident, the Russian hack of the Democratic National Committee, the suspected theft of billions of dollars of American intellectual property by China, the shutdown of the Ukrainian power grid by hackers, and the tens of thousands of cyber attacks we face every year, it is clear that all levels of government and private industry need to get serious about cyber security and start proactively protecting themselves.

Virtually every aspect of our society is online and vulnerable to criminal attacks by anyone with an internet connection. Intellectual property, medical records, critical infrastructure including nuclear power plants, the power grid, water and sewer systems, airports, communications systems that allow for phone calls, text messages and emails, and many other critical components can be compromised by the smallest slip in security. The Russian hack of former White House chief of staff John Podesta's Gmail account is the perfect example. Hackers sent him a fake Google password reset page, aka a phishing attack, and he took the bait. If this had happened at a nuclear power plant, the hackers could theoretically cause a meltdown.

"Public and private organizations need to take a holistic approach to their security posture," said Scott Johnston, president of the Miami-based firm JohnsTek, whose founders have worked at the highest levels of the U.S. government's cyber security and Homeland Security organizations.

"It's not just about locking your doors at night and turning off the computers. Bad actors exploit security gaps in an organization's policies, business processes, and network activities to gain access to sensitive data or control user accounts. The results can be devastating."

Fortunately, many are starting to act, and as a result cyber security jobs are in high demand. There are currently 209,000 unfilled cyber security jobs in the USA alone. By 2019, this shortfall is expected to drastically increase to 2 million jobs. Technology is a major part of every aspect of modern life, and filling these jobs or contracting with third-party security providers will be a big step toward defending our homeland.

The Miami Beach incident is merely one example of exposed vulnerabilities. Rest assured, many more of these vulnerabilities will be discovered, and the next attack could be far more lethal. Breaches in security coverage are a major threat to our way of life, and it's imperative that local leaders implement a comprehensive security posture to protect their organizations and our infrastructure, sensitive data, and revenue from these 21st century threats.

There are plenty of ways to protect ourselves, but remember, our society is currently vulnerable and hackers are lurking.

Andrew M. Korge is the vice president of strategic development at the Lynx Companies, which has multiple portfolio companies in real estate and technology, including JohnsTek, Inc., which engineers strategic solutions uniquely designed to protect government and business assets on the ground and in cyber space.

This article is related to: Cyber Crime, Crime