Usually, impersonations are funny. When a criminal poses as a CEO of a company via email and directs employees to wire hundreds of thousands of dollars—sometimes millions—into an account overseas, it’s anything but.

You would think impersonating a CEO would be difficult. According to James Barnacle, chief of the FBI’s money laundering unit, “It’s as easy as having a computer.” Business email crime, also known as CEO Email Fraud, is an up and coming version of identity theft that has increased dramatically over the last three years. In fact, between October 2013 and August 2015, about $1.2 billion globally was lost to CEO Email Fraud.

The rise in CEO Email Fraud can largely be attributed to one simple fact: the scam can be run from literally anywhere in the world where there’s an Internet connection. Criminals looking to swindle companies out of large sums of money often use look-alike domain emails that are unlikely to set off spam traps. They also take the time to understand the target organization’s relationships, activities, interests and travel and/or purchasing plans, allowing them to mimic the CEO’s mannerisms more easily.

In addition to the scheme being relatively easy to execute, the money often ends up in offshore bank accounts located in Asia or Africa, where it’s harder for the U.S. to acquire assistance from local authorities. The FBI advises companies to be more guarded with their information, even if it means taking additional steps that are not cost-effective.

Also recommended is being aware of the latest version of CEO Email Fraud. The most recent being urgent requests from criminals posing as CEO’s asking employees to send them copies of their W-2’s. These documents are a gold mine of personal information and, since employees aren’t likely to question a request from the head of the company that pays their salary, relatively easy to obtain in these cases. The unfortunate reality of CEO Email Fraud is two-fold: Not only does it put employees at risk for identity theft, but it also puts companies at serious risk for financial loss.

To prevent falling victim to these scams, make sure both Accounting and Human Resources are aware of what CEO Email Fraud is and how it works. Encourage employees to check email addresses and confirm directives by asking before acting. Minimize risk by trusting Mackinac Partners to put preventative measures in place within your network systems. Using our extensive suite of Business Intelligence and Corporate Security services, our experts will work with your IT department to create checks and balances so that employees can make better informed business decisions, protecting themselves — and the company — from ongoing risk and challenges.

To learn more about our services, visit us online. If you have questions, or would like to set up a consultation, contact our team of professionals and we’ll get back to you within 24 hours.