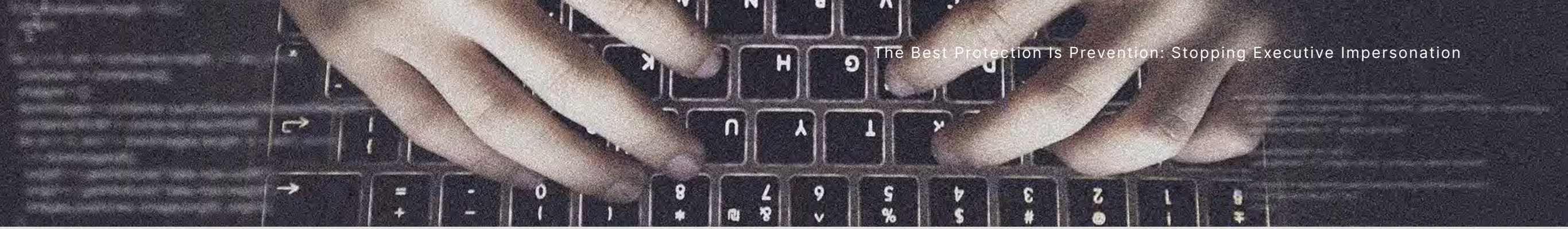




# **The Best Protection Is Prevention: Stopping Executive Impersonation**





CEO or executive impersonation is exactly as it sounds. A nefarious phisher or scammer poses as an executive, managing director or other senior figure and attempts to have payments made from within the organization to a third party. Sometimes this is known as business email compromise, a \$26 billion scam according to the FBI<sup>1</sup>.

### Picture This:

Someone in your organization has just received an email, phone call or LinkedIn message from what looks like you or your CFO. “Quick,” it says, “we missed a big payment to one of our vendors and we need to fix it.” It’s fair to assume that as the boss, when you need a mistake fixed, your employees will get on it—and fast. Hey, it’s why you hired them in the first place. But what if that communication was spoofed almost indistinguishably to look and sound like you, or worse yet, your real account hacked? It happens more often than you think.

### How Mattel Nearly Lost Millions

The year was 2016. The target was LA-based toy company Mattel. The Barbie Doll manufacturing machine had just hired a new CEO named

Christopher Sinclair. Chinese hackers did their homework, researched the company, employees, payment processes and executive clearance levels. Spoofing Christopher Sinclair’s email, cybercriminals targeted a senior finance executive who possessed the ability and authority to approve large cash transfers. The impersonators asked for a deposit to the Bank of Wenzhou, China where uncoincidentally Mattel was preparing to expand their operations, so nothing seemed out of the ordinary. Three million dollars was sent. Ch-ching? More like uh-oh.

The finance executive went on to mention the transfer to Christopher Sinclair in conversation not long after, only to discover they were victims of an elaborate phishing scam. Fortunately, the story ends well for Mattel. With a little bit of luck and a long weekend Bank holiday, the FBI had time to work with Chinese officials to recover the stolen funds. But that’s not always the case. Since the incident in Wenzhou, Mattel has tracked a dozen more attempted hacks<sup>2</sup>.

<sup>1</sup> <https://www.ic3.gov/Media/Y2019/PSA190910>

<sup>2</sup> <https://www.cbsnews.com/news/mattel-vs-chinese-cyberthieves-its-no-game/>

## Bogus Invoices & Billions of Dollars

Between May 2018 and July 2019, there was a 100% increase in losses due to these kinds of scams. They've been reported in all 50 states and in 150 countries.

A Texas-based energy company was also defrauded out of \$3.2 million<sup>3</sup>. A cybercriminal impersonated the CEO and tricked an executive assistant into paying a bogus invoice. He had done his research, getting the assistant's name and address off the company's own website. He was convincing enough to gain the assistant's trust by mentioning details he had learned about the CEO through Facebook. Remember, the devil can be in the details.

In a separate incident in the UK, an executive was conned in an even more disturbing fashion<sup>4</sup>. A cybercriminal used AI-generated audio to impersonate the CEO's voice. The targeted executive transferred \$243,000 to a fake supplier. This is what's called a deep-fake and can be dangerously convincing.

<sup>3</sup><https://insights.sei.cmu.edu/blog/business-email-compromise-operation-wire-wire-and-new-attack-vectors/>

<sup>4</sup><https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/>



A Texas-based energy company  
was defrauded out of  
**\$3.2 MILLION**



**100%**  
increase in losses  
due to scams between  
May 2018 and July 2019



“Cybercriminals can attack your customers, your employees, or your brand outright without ever targeting your infrastructure.”

## Protection Through Prevention

Is all hope lost? Of course not. Protecting yourself and your organization from business email compromise is entirely possible. It’s important to educate yourself and your employees on how these kinds of scams are performed and what methods phishers will use, but the burden doesn’t need to fall entirely on you.

Remember, cybercriminals can attack your customers, your employees, or your brand outright without ever targeting your infrastructure. And traditional security measures are unable to identify these types of attacks. You need real-time monitoring and notifications to prevent attacks before they become one of the cautionary tales above.

## Supercharging Brand Protection With Intelligence

Recorded Future’s Brand Intelligence Module is the helping hand you need. Security teams can be in more places at once, monitoring, detecting and translating threat behavior so you don’t have to.

Recorded Future’s unique collection approach aggregates data across the broadest set of sources across the Internet, including data from domain registrations, dark web channels, and social media sites. With brand intelligence, security teams can instantly alert on things like, leaked credentials, typosquat domains, social media accounts meant to impersonate an employee, malicious logo usage, fake company applications, threats to executives and more.

Recorded Future’s machine learning and natural language processing reads the language of cyber threats and does the translating for you. So you can spend more time focusing on work and less time worrying if someone is impersonating you on social media. Bundled takedown services then help to simplify the process of removing malicious content.

## Brand Intelligence in Action

That's a lot of talk. Here's what it all means in practice.

With your executive cyber protection you can:

- Set up alerts for executive impersonation of your CEO on social media.
- Set up geofence monitoring across several cities where he or she travels regularly.
- Be alerted via email or the Recorded Future Mobile App when this alert triggers and easily pivot into Intelligence Cards for additional context on the threat.
- Take immediate, confident action to mitigate risk and keep your CEO out of harm's way.

Remember in Texas when the administrative assistant was tricked with personal details? That's where Brand Intelligence comes in. With Intelligence from Recorded Future you can rest assured that even though imitation is the highest form of flattery, it won't be costing your company millions of dollars.

## Take Advantage Of These Big Time Benefits

Security teams instantly gain complete visibility into threats that were previously difficult or impossible to identify. With Recorded Future, organizations can:

- **Identify threats 10x faster**
- **Identify 22% more threats before impact**
- **Boost overall security team efficiency by 32%**





#### **About Recorded Future**

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at [recordedfuture.com](https://recordedfuture.com) and follow us on Twitter at @RecordedFuture.