

# Whaling Fraud Rises in Finance Industry

A reporter once asked notorious criminal Willie Sutton why he robbed banks. “Because,” Sutton is said to reply, “that’s where the money is.”

The quote itself is probably apocryphal; violent criminals are not known for their cozy relationship with the press. But the story makes a relatable point because, as history has shown, criminals particularly like to rob banks. Well over a century later, today’s criminals continue the tradition. While some cybercriminals launch mass-mailing campaigns or target staff, others go where the money is.

It’s called “whaling,” and the target is (your) company executives.

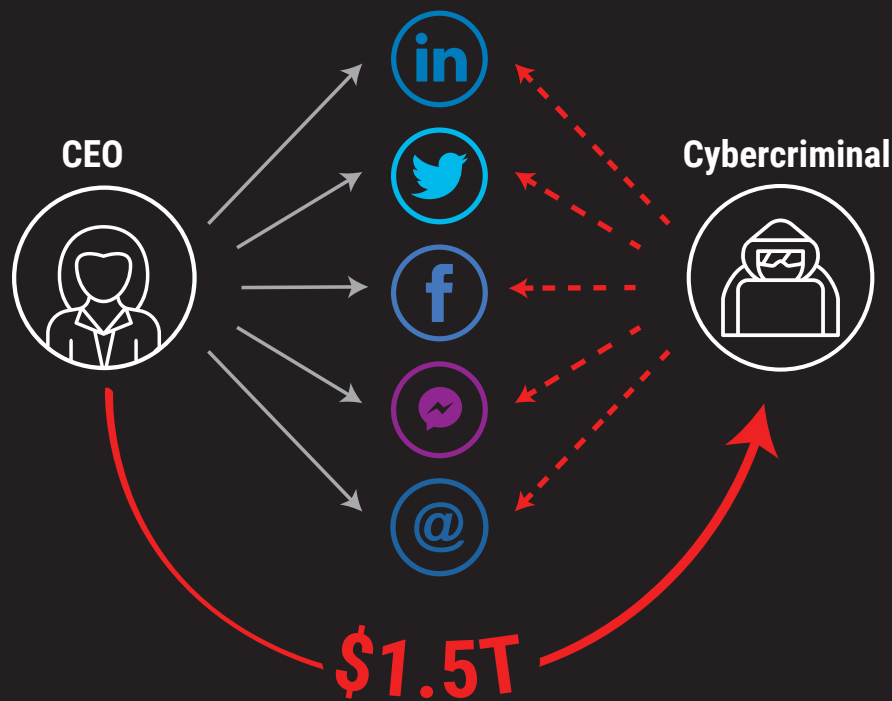
—

Nov, 2020 | Brandshield Data Center



# What Is Whaling?

## The Whaling Playground



Whaling is a form of spear phishing attack which targets the executives, key holders and other members of a company's leadership team.

While spear phishing goes for a specific type of target, usually employees of a hand selected organization, whaling focuses on landing a high-ranking executive, for example, the CEO of a major business. This typically involves far more research and work to ensure that the message hooks its target.

Also known as "CEO fraud" or "executive fraud," a whaling attack targets a company's top ranks. It's an attack on the big fish, or "whales," of your organization. The goal is to pursue someone with access to an organization's critical information, access or trust.

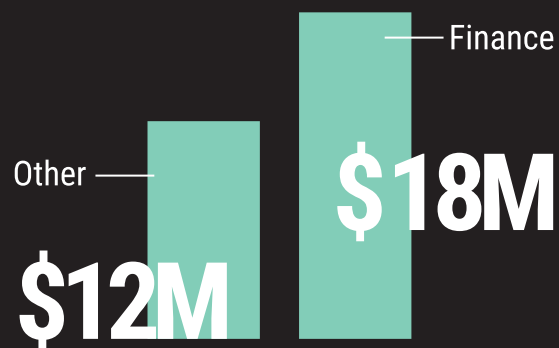
In recent years cybercriminals have begun to particularly rely on whaling attacks to compromise targets in the financial industry. Banks and many other finance companies build their security with layers or a tiered approach, with multiple identity and authorization checks in place. This means that accessing through a phishing attack targeting a bank teller (for example), will only take the threat actor so far, before being blocked.

Threat actors need the kind of access that your executives can provide and so they build their attacks accordingly. It works so well that, according to estimates by the Financial Times, whaling has cost the finance industry more than \$12 billion over the past several years. Other estimates suggest that number may be far higher, with banks alone reporting more than \$16.7 billion in losses in one year alone.

# Whaling Attacks Target Finance Executives for Their Access

CEO fraud works by either deceiving the targeted executive or posing as them. In the former case, a cybercriminal will attack your leadership directly. They try to trick them into giving up critical information, downloading malware or otherwise compromising your security.

In the latter case, a threat actor will attack your executive team by stealing their identities. They will pose as a company's leadership to your employees, clients and other third parties, seeking to steal materials in their name. This is what happened to Crown Bank, a U.S.-based institution, when a group



Cyberattacks cost financial institutions \$18m compared to \$12m for any other company

Source/ Accenture: Cost of Cyber Crime Study.

of cybercriminals posed as the wife of bank CEO, Jacinto Rodrigues. Under this stolen identity they sent 13 e-mails to bank employees requesting financial transfers that totalled more than \$2.7 million. Although recipients did some of their due diligence, they didn't follow up by telephone or in person when these emails asked

Cyberattack  
Industry  
Target Ratio

Finance Vs. Non-Finance

300:1  
Attacks Attack

Source/ Boston Consulting Group: Global Wealth 2019: Reigniting Radical Growth

for increasing wire transfers to an account in Singapore. Who would when dealing with the wife of the boss?

Problem was, that the email didn't come from Jackie Rodrigues.

Whaling depends on many of the elements that causes a company to function in the first place. The trust and access you invest in your leadership (and in yourself) allow the company to flourish, but they give those same decision makers the keys to your kingdom. The chain of command that enables your company function smoothly can also prevent employees from vetting requests that appear to come from the top. This is a danger for any industry, but the finance industry faces an entirely different magnitude of risks.

Whaling and phishing attacks target financial institutions 300 times more often than any other business category

This volume of attacks makes whaling particularly dangerous. Unlike a scheme, whaling attacks only need one successful message to profit millions. How many messages does a threat actor need to send before that one slips through?

# How Do Whaling Attacks Work on Financial Institutions?

When Belgium's Crelan Bank was attacked, the first sign anyone had was an email claiming to be from the CEO asking staff members to wire more than \$75 million to a third party. Unfortunately no one at the bank knew they were under attack until after the money was transferred. This is all too common when it comes to CEO fraud.

Whaling works like most targeted ("spear") phishing. Often attackers will take their time and research their target in advance. They gather information from social media, company web pages and even third parties to learn more about your executives and build a crafted message.



Numbers of attacks per time unit for financial institutions

**30/second**

**2.6M/day**


**~1B/year**



 **FBI:**

CEO Fraud Yearly  
Valued At **\$26B**

**100%** Increase  
in 2019.



Criminals bombard financial institutions with cyberattacks like these and others, launching 30 new attacks on every company every second of every day. Your company can face more than a billion attacks per year. Just a single whaling attack has to get through for a multi-million dollar jackpot, and modern cybercriminals have a terrifying 20 percent success rate against even hardened systems.

A direct attack will often try to co-opt sources that your leaders trust. The threat actor might, for example, impersonate a co-worker on social media. They may learn your executives' habits and set up a copy of frequented websites, perhaps even your own, duplicating brand

identity and logos to create the impression of a trusted portal. They even may pose as a potential client, co-opting the identity of other businesses (perhaps through a successful whaling attack on those third parties).

The goal is always the same: trick your leadership into lowering their guard and trusting the threat actor's identity.

A threat actor who wants to steal your leadership's identity will try many of the same tricks in reverse. Instead of setting up a Facebook account to look like your CFO's friend from college, they will set up a page for your CFO themselves. They will research your executives'

habits and relationships to craft messages that sound authentic and will not hesitate to use any information they can get to try and sell their deception.

Say, for example, your CTO periodically takes members of the sales team out for lunch. Now say a member of your sales team posts about that afternoon's lunch on Instagram. A cybercriminal might seize on this, writing an e-mail with a line like "glad you enjoyed the steak house today, let's do it again soon!"

The punchline feels too spontaneous to be a lie, which is the whole point.

# How to Protect Financial Institutions Against Whaling



Now, that you are aware of this rising phenomenon and the way threat actors spread their malware or phishing hooks, and how it threatens your company, what's left is to protect your company from whaling attacks and CEO fraud.

Defending yourself against CEO fraud starts by protecting your executives in the same way you protect your brand. Their identities are targets, the same way cybercriminals target your company and for much the same reason.

Don't wait to accidentally find an attack or catch one in progress. Approach this matter as you approach other cyber threats, by integrating the proper detection and active remedies. In particular, the best defense combines effective training, smart technology and strong legal capabilities.

First, compose a list of your company's high-profile executives, starting with the CEO. These names should be considered corporate assets, the same as corporate logos, trademarks and patents. Use this list to adopt a proactive approach, with an emphasis on monitoring for fake social media accounts. The damage caused by links published on behalf of the CEO's impersonator can mount to millions of dollars, and your executives need to learn how to protect their identities while online.

Today more than ever leadership and staff alike need to check carefully when they receive unsolicited messages, even from within the company. That's particularly important when it comes to messages sent over social media. While your IT team can control what passes through their mail server, third party platforms are another story altogether.

This isn't just about training. Eventually technology has to fill in the gap, solutions that your executives and customers won't have.

Cybercriminals set up websites and social media accounts that borrow the identities of your company and its leadership. They steal your logos, branded content and even corporate photos to pull this off. That makes those fake accounts convincing, but it also makes them vulnerable. The right tools can detect these stolen images, and early detection of look-a-like pages can stop them.

Online threat hunting is the ability to not only monitor and detect whaling attacks. It is essential to protecting your company, but once you find the threats you will need to stop them and take those threats down. That's where legal expertise enters the picture.

You will need to work with social media companies to take down fraudulent profiles, and with hosting services to remove fake websites. Traditional cybersecurity can go part of the way, but this process requires experience and a team built to integrate the technical side of security with your legal team.

Building that kind of workflow and strong communication across dramatically different teams can prove to be quite a challenge, but it's worth the effort.

## **Technology & Expert**

Of course, there are 3rd party cybersecurity solutions with robust technology and legal expertise that provide a complete solution from detection to takedown, enabling you to gain control over this issue and remove threats quickly and efficiently before the real damage is done. Utilize the experts to connect cybersecurity and legal to a successful whaling protection.

# Online Phishing & Fraud Landscape Finance Industry: Dec 2020



## Sources

- Boston Consulting Group: Global Wealth 2019: Reigniting Radical Growth
- Accenture: Cost of Cyber Crime Study.