

Exhibit 2025

[← Back to blog](#)

usecure

[usecure Homepage](#)

[Login »](#)

[Phishing](#) [Scams](#) [In the News](#)

The 7 most damaging phishing attacks of all time



Micke Ahola



The most damaging
phishing attacks
of all time

Phishing emails are used to steal money and sensitive information from businesses every day. While any scam can be damaging, some far exceed others in the value of damage that they cause to their target.

Some [phishing scams](#) have been known to be involved in the theft of tens of millions of dollars. Others have been used to release sensitive military documents, or take down an entire power grid. But what are the worst phishing attacks of all time? Find out in our ranking below.

The 7 most famous phishing attacks

7. Ubiquiti Networks loses \$39 million to CEO Fraud (2015)

CEO Fraud is one of the most dangerous types of phishing. It involves a cyber criminal posing as a senior executive (usually the CEO) of a company, and asking an employee to handle an urgent money transfer.

Since most employees wish to appear responsive in the eyes of their senior management, it is easy for an employee to fall for one of these emails and send large sums of money to the wrong recipient.

In 2015, an employee at Ubiquiti Networks in California was involved in one of the worst CEO fraud cases of all time - losing the company [\\$39 million dollars](#) as a direct result of the scam.

6. Austrian aeronautics company loses \$42 million to CEO Fraud (2016)

Fischer Advanced Composite Components AG, an Austrian aeronautics company, was another high-profile victim of a CEO fraud scam.

In 2016, an employee in Fischer's financial department received an email impersonating the company's CEO Walter Stephan. The employee then

proceeded to transfer **almost €50 million euros** to a cyber criminal's bank account.

The company was able to recover around €10 million once other employees realised the scam had taken place - but the rest of the money was lost.

5. Drugs company in Minnesota loses \$50 million to spoofed email (2016)

Upsher-Smith Laboratories in Maple Grove, Minnesota, is another recent victim of a CEO fraud scam. An employee paid out over **\$50 million** over a series of transactions to a number of bank accounts in the cyber criminal's control without raising any red flags.

There is now an ongoing criminal lawsuit between Upsher-Smith Laboratories and their bank over who is going to pick up the bill for the damages. The laboratory claims that the bank missed multiple red flags - ones its own employees missed as well - and should take some responsibility for the lost money.

4. Belgian bank loses \$70 million to phishing scam (2016)

Phishing scams target businesses across the world, and institutions that often carry out high-value financial transactions, such as banks, are some of the most desirable targets.

While fraud checks and anti-phishing staff training is highly prevalent in most banks, it is still possible for employees to mistakenly expose money to cyber criminals.

Belgian bank Crelan was hit by a phishing email that convinced an employee to send over **€70 million** to unknown bank accounts - a mistake they're not likely to repeat.

3. RSA Security: the phishing email that took down the experts (2011)

A well-timed and carefully crafted phishing email can fool anyone. That was proven in the RSA Security hack of 2011, where network security experts contracted by the US Defence department to provide security solutions [fell for a phishing email](#) themselves.

Little is known about what information was revealed in the RSA breach, and for understandable reasons the company and the US Defence department have kept information about the breach under a tight seal. Still, as a hack that penetrated the experts themselves, the RSA breach has become one of the most famous phishing scams.

[2. The fake invoices that cost Google & Facebook over \\$120 million \(2013-15\)](#)

In 2017, Lithuanian authorities arrested a man by the name of Evaldas Rimasauskas. The accusation he was arrested for was quite extraordinary: he had purportedly sent fake invoices to large companies including Google and Facebook for a period of years, stealing [over \\$120 million](#) in fake payments arriving in his own bank accounts.

In large companies, financial departments often handle thousands of transactions in a single day. Thus it is easy for an outsider to slip in an invoice that looks the same as any other at first glance - and receive a payment in their own bank account.

The authorities were able to regain about half of the money lost in the scam, but the attack highlighted just how important it is for employees in financial departments to receive the right training to spot fake emails.

[1. The phishing attack that took down Ukraine's power grid \(2015\)](#)

The most famous phishing attack of all time is the one that [took down Ukraine's power grid](#) in 2015, leaving hundreds of thousands of people without electricity during a cold winter's night.

The attack had devastating consequences for businesses and individuals across the country, and involved a months-long campaign of spear phishing emails used to steal credentials and information from systems administrators and officials.

Ukraine was quick to point its finger at Russia as the attack created a blackout across much of the country. While the perpetrators of the attack have never been revealed, the attack is ominous in its relation to the current invasion of the country by Russia, seven years later.

Keep your users safe from phishing emails - and protect your company's money

User training is absolutely essential to reduce the chance of employees falling for phishing emails. Without the right training regime, any employee can give up sensitive information that opens the company up to a major breach.

In addition to training, employees should be regularly tested with realistic simulated phishing emails. These simulations help users learn to spot phishing emails in their own inboxes, and encourages them to stay alert for phishing at all times.

[usecure](#) is your full-fledged Human Risk Management solution. Learn more about how you can reduce user risk with regular training and testing below.



usecure Demo Hub

Learn how usecure builds a security-savvy workforce

Understand how usecure can help you monitor and reduce human cyber risk through quick on-demand demos.

[Go to Demo Hub >>](#)

The advertisement features a dark blue background with a grid of small white dots. On the left, there is a circular inset showing a man in a light blue shirt. Next to it is a screenshot of the usecure Demo Hub interface, which displays various security-related charts and data. A green arrow points from the man's head towards the interface. Another green arrow points from the bottom left of the interface towards the right. In the bottom right corner, there are three small green dots.



[Crypto Scams Industry CEO Blog](#)

The rise of Crypto scams and how to avoid being fooled

Everyone should be into crypto, right?

I mean, why not, it's the newest and most secure way to transfer money.

Bitcoin has been around in the world long enough that...



Charles Preston

[Blog »](#)



Phishing

How to create a well-crafted phishing simulation that truly tests employee response

Cyber criminals have a number of tricks up their sleeve that they use to get their unsuspecting victims to click on the links in phishing emails.

Here's how you can...



Micke Ahola

[Blog »](#)

Platform

Security Awareness Training

Simulated Phishing Software

Simplified Policy Management

Resources

2021 Guide to Security Awareness

Launch a Free Phishing Simulation

Security Awareness Videos

Company

Homepage

Contact

Help Centre

Book a Live Demo

Work email address...*

Choose a Time »

in

