

Exhibit 2024

The Worst Phishing Attacks in History

January 05, 2023



The internet has been one of humankind's most prominent developments, completely transforming our lives in a myriad of ways. It is the magic wand that has brought a plethora of services, information and opportunities to our fingertips. However, we don't live in a perfect world, and the world wide web also has its share of stumbling blocks. One of the most significant drawbacks of the internet is phishing. While some attacks go unnoticed, leaving organizations relatively unscathed, many phishing scams [have a lasting impact](#), which results in severe financial and reputational damage. However, some phishing attacks are big enough and damaging enough to make history.



Get the guide that helps you detect & defeat dangerous BEC attacks to keep your company out of trouble! [DOWNLOAD IT >>](#)

The 5 worst phishing attacks in history

[Phishing](#) is at the root of many of the most devastating cyberattacks, including business email compromise schemes that cost companies millions. Here are some attacks that will forever be etched in history for their devastating impacts.

The Facebook and Google scam

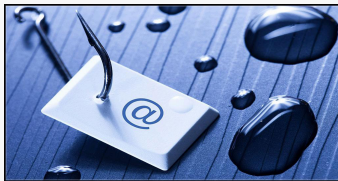
In this classic case of [business email compromise \(BEC\)](#), a Lithuanian man named Evaldas Rimasauskas stole over \$100 million from Facebook and Google. Rimasauskas and his co-conspirators created fairly convincing forged email accounts of Taiwan-based Quanta Computer, which actually does business with Facebook and Google. They sent carefully crafted phishing emails with fake invoices, contracts and letters to employees at both these tech giants, falsely billing them for millions of dollars over a period of two years between 2013 to 2015. The [Facebook and Google employees paid more than \\$100 million](#) to Rimasauskas' fake company's bank accounts, which he reportedly laundered through banks in Latvia, Cyprus, Slovakia, Lithuania, Hungary and Hong Kong.

The NotPetya malware attack

In June 2017, the world woke up to the most devastating cyberattack in history that spread across the planet like wildfire, ushering in a new era of cyber warfare. NotPetya initially started as a supply chain attack against Ukrainian companies through updates from a small Ukrainian accounting software company. However, it quickly spread to more than 60 countries, affecting the computer systems of thousands of multinational companies.

NotPetya comes from the family of Petya [malware](#) that targets Windows-based systems, infecting the master boot record to execute a payload, which encrypts a hard drive's file system table and prevents Windows from booting. Once cybercriminals encrypt the file system, they demand a ransom in Bitcoin to decrypt the files. However, while the Petya malware is typically the province of everyday cybercriminals, NotPetya is widely regarded as a state-sponsored Russian wiper malware masquerading as ransomware. Petya malware allows the victims to decrypt their machines after payment, but NotPetya destroys making it almost impossible to retrieve.

The NotPetya attack ensnared many companies, including Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, Saint-Gobain Mondelez and Reckitt Benckiser. The [monetary damages caused by the malware was pegged at more than a mammoth \\$10 billion](#) – the most significant in the history of cyberattacks.



Learn the ins and outs of today's wide variety of phishing attacks & how to stop them in *Phishing 101*. [DOWNLOAD IT >>](#)

Ukrainian power grid attack

In December 2015, a Ukrainian electricity distribution company, Kyivoblenergo, became the world's first power grid provider to be taken down in a cyberattack. The threat actors were able to attack the Ukrainian electric utility company and force a blackout [through a phishing email](#) that enabled them access Kyivoblenergo's network.

Using malware known as BlackEnergy, the perpetrators were able to attack the company's computer and SCADA systems, disconnecting 30 substations three hours. Widely perceived as an attack by the NotPetya scammers, [as many as 230,000 customers lost power](#) – almost half of the homes in the Ivan Frankivsk region in Ukraine, which has a population of about 1.4 million.

Ubiquity Network social engineering attack

In another BEC scam, a San Jose-based technology company, Ubiquity Network, was subjected to a whaling attack on June 5, 2015. [Impersonating a senior member of the company](#), the scammers sent an email to a member of staff in the financial department of the company's subsidiaries based in Hong Kong who fell prey to the scammers' scheme. The attackers impersonated the company's CEO and lawyer and instructed the company's Chief Accounting Officer to make a series of transfers to close a secret acquisition.

Over the course of 17 days, the company made 14 wire transfers to accounts in Russia, Hungary, China and Poland. The company reported transfers of funds totaling an estimated \$46.7 million that was held by the company's subsidiary incorporated in Hong Kong to other overseas accounts. The scheme only came to light after the U.S. Federal Bureau of Investigation (FBI) contacted Ubiquity to inform them that the agency suspected that the company had been a victim of fraud.

FACC business email compromise attack

Austrian aerospace parts manufacturer and engineering company FACC fell victim to one of the most financially damaging [BEC attacks](#) in history in 2016. In this incident, an employee at FACC received a seemingly routine email in which bad actors posed as the company's CEO and asked the organization to transfer an estimated \$50 million to another account as part of an "acquisition project." The message appeared to come from FACC CEO Walter Stepha and the employee fell for the bait, transferring the money. The company was able to prevent about \$10 million from being transferred at the last minute, the damage was severe, and FACC's CEO lost his job as a result.



Learn how incident response planning boosts cyber resilience & security. [GET THE EBOOK >>](#)

Protect your organization from phishing attacks with Graphus

[Graphus](#) is the world's first AI-driven email security solution that automatically protects organizations from email-based phishing attacks, including ransomware, BEC and others. The patented AI technology of Graphus put multiple layers of defense between organizations and phishing emails, mitigating attacks before they reach employees. It analyzes communication patterns between people, devices and networks to reveal untrustworthy emails, making simple, powerful and cost-effective automated phishing defense solution for companies of all sizes.

- Graphus blocks sophisticated phishing messages before users see them.
- Puts three layers of protection between employees and dangerous email messages.
- Seamlessly deploys to Microsoft 365 and Google Workspace via API without email traffic rerouting or lengthy installs.
- Provides intuitive reporting to help you gain insights into the effectiveness of your security, level of risks, attack types and more.

If you wish to learn more about Graphus, book a demo [here](#).

Stay safe from even the most sophisticated cyberattacks and social engineering scams

Put the powerful TrustGraph® AI of Graphus to work for your business, and in minutes you'll get a powerful, easy-to-use, and customizable EmployeeShield® against phishing attacks.

[Get a Demo of Graphus](#)

[« Previous](#)

[Next »](#)

RECENT POSTS

[Email is Still the Most Concerning Cyber Threat Vector](#)

[Empowering Email Users: Introducing Graphus Personal Spam Filter](#)

[Email Phishing is a Real Nightmare for Businesses](#)

[Dangerous AI-Driven Phishing Attacks Are Headed to an Inbox Near You](#)

[Why Is Cyber Insurance So Hard to Get and What to Do About It?](#)

CATEGORIES

[Account Takeover \(ATO\)](#)

[Advanced Persistent Threats \(APT\)](#)

[Artificial Intelligence \(AI\)](#)

[Automation](#)

[Automation Protection](#)

[Business Email Compromise](#)

[Cyber Insurance](#)

[Cybersecurity](#)

[Dark Web](#)

[Data Breach](#)

[Email Security](#)

[Feature Overviews](#)

[Incident Response](#)

[Insider Threats](#)

[Malware](#)

[Managed Detection and Response \(MDR\)](#)

[Network Security](#)

[Password Management](#)

[Phishing](#)

[Phishing Simulation](#)

[Ransomware](#)

[Remote Working](#)

[Response](#)

[Sales & Marketing](#)

[Security Awareness Training](#)

[Social Engineering](#)

[Spam](#)

[Spear Phishing](#)

[Spoofing](#)

[Staffing & Recruitment](#)

[Supply Chain](#)

[Threats](#)

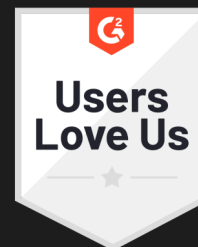
[Uncategorized](#)

[Zero Day](#)

Communicate with confidence knowing that your inboxes are safe from even the most sophisticated cyberattacks and social engineering scams

Put the power of Graphus AI to work for your business and get three shields of defense against phishing attacks and spam in minutes.

[Get a Demo of Graphus](#)



GRAPHUS

701 Brickell Ave Ste 400
Miami, FL 33131
sales@graphus.ai
(786) 530-5002

NAVIGATION

[Product](#)

[Success Stories](#)

[Resources](#)

[Blog](#)

FOLLOW US

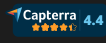
[!\[\]\(10f8862fc183b400327470ea85afe9ae_img.jpg\)](#) [!\[\]\(4ba8d838a2aa5445d51c9dee78fcb0cc_img.jpg\)](#) [!\[\]\(4fe307d00a844a23eb14d503e73187bd_img.jpg\)](#)

[Partner Portal](#)

[Request a Demo](#)

[Community](#)

[About](#)



©2024 Graphus. All Rights Reserved.

[Privacy Statement](#)

[Website Terms of Use](#)

[Edit Cookies Settings](#)