# Spearphishing a Whale

Spearphishing is a targeted form of phishing that seeks to approach a specific group of people for a specific purpose. Phishing is contacting people digitally to get them to engage with you, open an email attachment, click on a link, or some other malware-infected interaction. It’s always about gaining access to information like passwords and identification, usually with the intent of theft by fraud, using the acquired password and identification to access financial institutions or purchasing power online.

phishing is random but spearphishing is specific. Nothing illustrates that better than the newly released documentary, *Billion Dollar Heist*, available on Amazon Prime. It's a feature-length documentary that examines the 2016 theft of $81 million US dollars from the Bangladesh Bank, the central bank of the country. The targeted amount was $951 Million, hence the title, *Billion Dollar Heist.* If not for a single spelling error and the impatience not to persist another hour, there's a very high likelihood that the cyber criminals would have gained the 951 million.

The meticulously orchestrated heist, which took a year to plan, finalize, and execute, is a textbook example of how serious digital crime is now. Gone are the days of the basement hacker. In their place are sophisticated criminal organizations that are well-funded, organized, and capable of floating a payroll for a sustained period to be required to plan and execute a crime of this scale.

The heist was pulled off by the Lazarus Group, perhaps the most infamous cybercrime organization in the world, and certainly the one feared most by governments and corporations. It’s believed to be based in North Korea, which certainly lends to the idea that it is state-sponsored. In the last decade, they have been connected to the breach of the Sony Pictures Network, the Bangladesh bank heist, and numerous cryptocurrency heists. Their signature is their advanced technical capability, which includes the use of home-coded malware of a caliber very rarely seen, their incredible patience, and their corporate-level due diligence.

Despite the extraordinary complexity of the job, it began with one of the most common errors that people make, an error that should never be made by somebody working in a secure environment, and a central bank is the very definition of a secure environment. A spearfishing email was sent out seeking employment. It had one attachment, a resume. The people targeted to receive the email were scouted through social media. They were known to work at the Bangladesh Bank and they were deemed to be the most likely to open the attachment on the spearfishing email. This psychological profile was worked up by the Lazarus Group after studying many more employees at the bank.

Of the thirty or so emails sent to employees of the Bangladesh Bank, three of the recipients broke security protocols and opened the resume. There was nothing innocuous about it to the eyes of the recipients. It was a standard resume with extensive experience in the financial sector. However, every one of those employees at the Bangladesh Bank should have asked themselves why the email was coming to them in the secure section of the bank in which they worked as opposed to going to designated personnel in the human resources department. That was the red flag. The weakness of character that could not stay the curiosity to open the resume was probably determined by the extensive profiling on social media.

Attached to the resume, and triggered by the opening of it, was a sophisticated piece of malware that gained access to the general network of the Bangladesh Bank. Once that access had been gained, the Lazarus group patiently mapped the entire network. In most instances, a cybercriminal group would not be able to stay inside a network like this without being detected, but the Lazarus Group is more than capable of leaving no tracks. They were inside the network for an entire year before the heist was pulled, and it all began with the simplest of cybercriminal tactics, phishing, albeit spearphishing with the added component of psychological profiles derived from social media, not something a normal low-level cybercriminal would do, but this was a central bank they were going after.

Once inside the bank’s Network, they slowly began to map the entire network. When they found the routers they discovered that many of them were not segmented. This was a strategic weakness in the network configuration. From this router, they were able to find the terminal through which the bank did their Swift transactions. They spent months gathering intelligence. They waited for a combination of four days that would have the various Banks involved, which included the Bangladesh Bank, the New York office of the US Federal Reserve, and a recipient Bank in the Philippines, concatenate a series of religious and national holidays that would give the thieves four days before a significant security response would be mounted. These holidays included the Friday prayers for the Muslim country of Bangladesh, the Saturday and Sunday at the US Federal Reserve, and the commencement of Chinese New Year in the Philippines. One writing about network security does not need to complement criminals, but this heist was brilliant. It was like an unwritten Stephen Soderberg script that could have been added to the *Ocean’s Eleven* franchise. One of the vulnerabilities of network security is the fact that it is a network. Many of the world’s central banks transact with the US Federal Reserve. The security standards at most European central banks and the US Federal Reserve are second to none, but the same could not be said about the Bangladesh Bank. It was the weak link in the chain, and it was chosen specifically for its network security weakness, and because it is a network, where there is one weak link the entire network is weak. This was how the thieves were able to steal from the US Federal Reserve.

The money was ultimately routed to the bank in the Philippines, where they had an assistant manager at the branch in on the job. She may not have known what she fully signed up for, but she took money to open several accounts. When the money was transferred to the accounts she accepted instructions to have it loaded into boxes and transferred to a casino in Manila where it was laundered by gamblers. She was the only person to be convicted of the theft. She got a fifty-six-year sentence. The documentary is well worth watching, not just by interested viewers but by security professionals because it is one of the most compelling network security breaches in recent memory.

As compelling and dramatic as the overall story is, the real takeaway of the Bangladesh Bank heist is basic security protocols. The standard security measures to protect against fish[hishing are simple. The most important thing is to verify the sender of any attachments. If you don’t know the sender then don’t open any attachments. Be suspicious of anything that asks you to act immediately. As innocuous as it was, the resume sent to the employees at the Bank of Bangladesh was the perfect Trojan Horse. The people who received the resume were not in the correct department for hiring. There was no business need to open up the attachment. They violated the most basic of security protocols for simple human curiosity. Three employees opened the attachment of thirty plus who received it, around ten percent, an excellent success rate for the Lazarus Group. The next most important thing is never to download a suspicious attachment. This is especially true in work environments, but it also applies to your personal computer. You may not be a central bank, and you may not have 81 million dollars to steal, but you do have payment information, banking card numbers, and credit card numbers. If you get a suspicious email with a link, hover over the link to verify the URL. Use multi-factor authentication whenever possible. After the Lazarus Group entered the network with the malicious software, they were able to access all of the computers on the network, none of which had multi-factor authentication. One of the best forms of multi-factor authentication is hCaptcha. It ensures that anyone passing beyond a certain security line in your network is human because it asks them to identify things that no malware or non-human would be able to identify. And the final piece of advice for professional network security is to be cautious on social media. You don’t need to share all the details of where you work. This is where the Lazarus Group gathered all of their information for the spearfishing attacks on the Bank of Bangladesh. If you follow these basic security protocols you should be fine.