

## True Phishing Stories

### Example 1

In January 2009 Bryan Rutberg was tricked into providing the password to his Facebook account. He was likely the victim of a spear phishing attack. (See sidebar.) Rutberg suspects that he responded to an email that asked him to click on a link to his Facebook account. When he clicked on the link he was actually taken to a fake web page that looked like Facebook where he entered his username and password.

The attacker then took over Rutberg's account and sent messages telling his friends that he had been robbed and asking them to send money to Western Union's branch in London. Thinking Rutberg was in need of cash, his friend sent the money. Rutberg's friend was an indirect victim of phishing and a direct victim of a scam similar to the "Nigerian" or 419 scam. These scams are directed to "reliable and trustworthy" people.<sup>1</sup>

### Example 2

In another attack, thousands of bogus subpoenas from the U.S. District Court in San Diego were "served" by email on corporate executives. The email contained an image of the official seal from the court and contained a link, supposedly to download a copy of the entire subpoena. However, when a recipient clicked on the link, key-logging software was installed on the user's computer instead. This is called a "whaling" attack. (See sidebar.)<sup>1</sup>

### Example 3

In late 2004, Nancy and Dan Boyle got a crash course in phishing. The first e-mail appeared to come from Bank One, warning that Mrs. Boyle's account would be suspended unless she updated her information to meet the company's new anti-fraud measures. She clicked on the link that came with the e-mail and entered the data on the Web site. Then the money disappeared from her account.

After that, she got another message that looked like it came from eBay. It warned of fraudulent activity on her account and urged her to verify her details. She handed over her bank account number, Social Security number and her mother's maiden name

The police got involved, but the evidence trail ran cold after investigators traced the scam to "somewhere in Egypt."<sup>2</sup>

### Phishing

"Phishing" is a form of Internet fraud that aims to steal valuable information such as credit cards, social security numbers, user IDs, passwords, etc.

-----

### Spear Phishing

"Spear phishing" is targeted communication toward employees or members of a certain organization or online group. Emails are customized with information publicly available on web sites like Facebook or MySpace. The emails then direct people to a fake login page.

-----

### Whaling

"Whaling" is phishing that is targeted at corporate executives, affluent people and other "big phish." Like spear phishing, whaling emails often are customized with information directed to the recipient (name and other personal information) and sent to a relatively small group of people.

1 [http://www.antiphishing.org/sponsors\\_technical\\_papers/DigiCert\\_Phishing\\_White\\_Paper.pdf](http://www.antiphishing.org/sponsors_technical_papers/DigiCert_Phishing_White_Paper.pdf)

2 <http://www.washingtonpost.com/wp-dyn/articles/A59349-2004Nov18.html>