Phishing attacks

phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

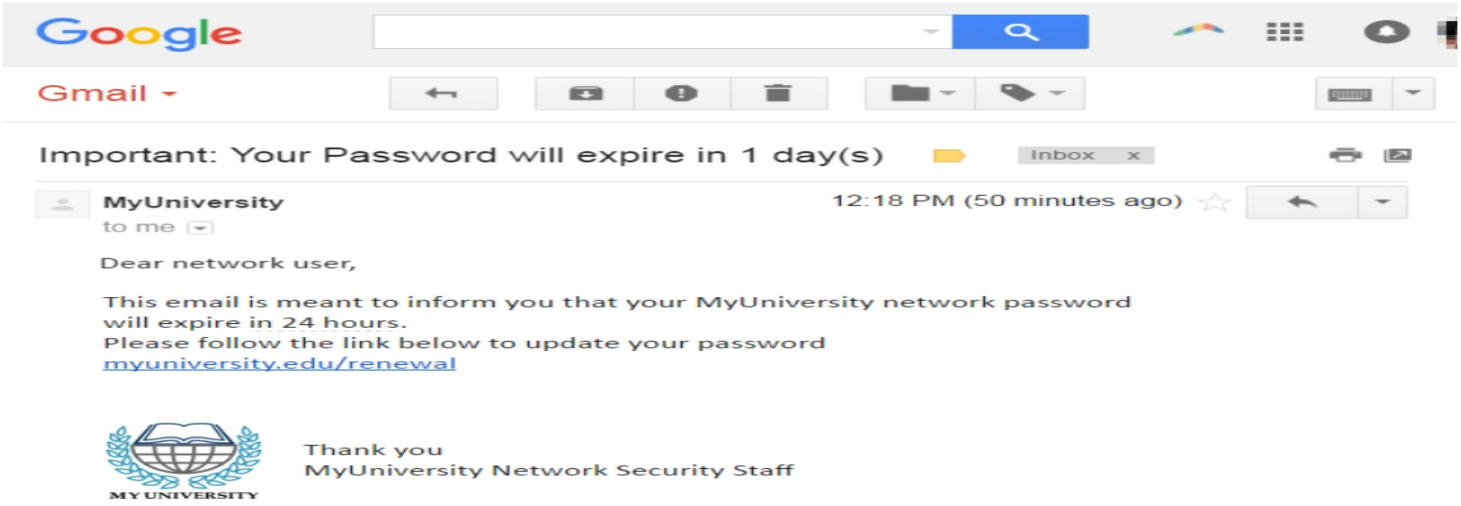
An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

Phishing attack examples:

The following illustrates a common phishing scam attempt:

A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.

The email claims that the user's **password** is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their **password** within 24 hours.



Several things can occur by clicking the link. For example:

The user is redirected to myuniversity.edurenewal.com, a bogus page appearing exactly like the real renewal page, where both new and existing passwords are requested. The attacker, monitoring the page, hijacks the original password to gain access to secured areas on the university network.

The user is sent to the actual password renewal page. However, while being redirected, a malicious script activates in the background to hijack the user's session cookie. This results in a reflected XSS attack, giving the perpetrator privileged access to the university network.

Email phishing scams:

attackers will usually try to push users into action by creating a sense of urgency. For example, an email could threaten account expiration and place the recipient on a timer. Applying such pressure causes the user to be less diligent and more prone to error.

Lastly, links inside messages resemble their legitimate counterparts but typically have a misspelled domain name or extra subdomains. In the above example, the myuniversity.edu/renewal URL was changed to myuniversity.edurenewal.com. Similarities between the two addresses offer the impression of a secure link, making the recipient less aware that an attack is taking place.