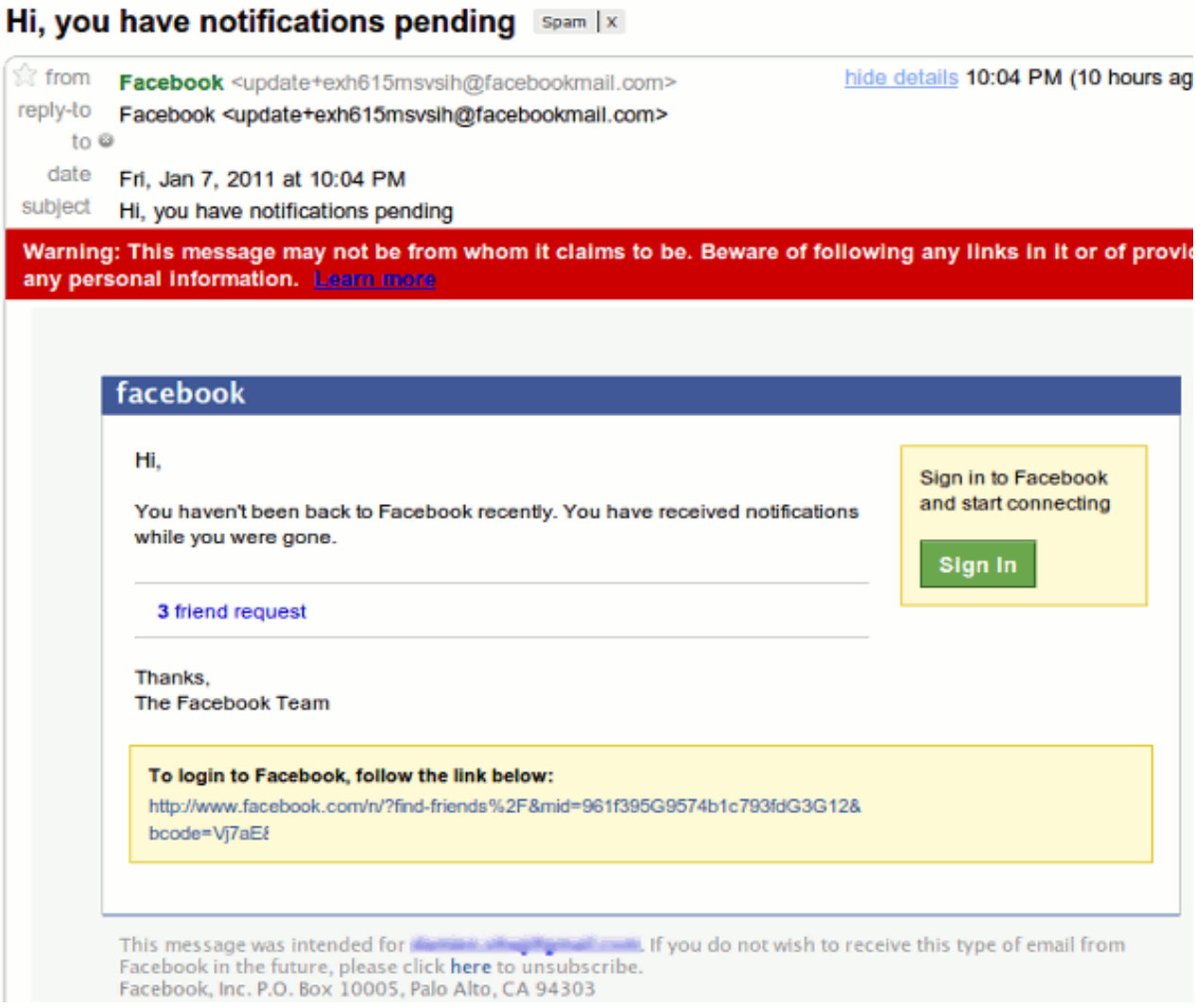
How Email Phishing Works and Why Clicking That Unknown Link Can Be A Dangerous Act.

Fishing can be a really enjoyable activity. But, getting fished, or phished for that matter, is not so fun. Yes, it is actually possible for people to get phished. Just like how fish that are fished are lured and killed, people who are phished are deceived and victimized. What exactly is phishing? Phishing is the act of deceiving (usually through email) people to reveal sensitive information such as passwords, bank account numbers, social security number, and credit card information.

With such sensitive information online, the stakes are obviously high. Sadly, as dangerous as they are, phishing attacks are common – very common. The 2012 RSA online fraud report indicates that there is an average of 33,000 phishing attacks each month; and these are just the ones reported. Because phishing attacks are so dangerous and prevalent, it is definitely important to protect yourself from them. This guide shows you how phishing attacks work and how to protect yourselves from them.

How Phishing Attacks Work

The main objective of phishing scammers is to steal information. To do this, hackers determine what information they need and how to retrieve it. They usually do this by sending you counterfeit or fake emails that seem to be from a legitimate company like Face book, and LinkedIn or any Bank in Uganda. In a majority of cases, they tell you that you need to update your personal information for security purposes. Here is how one phishing email might look like:



Exceptionally aggressive spammers may even tell you that your account will be permanently deleted if you don't update your information. Such scare tactics may indeed move you to give out your personal information. This is why many people are victims of identity theft. Here is an example of a phishing attack process:

1. You receive emails that seem to be from a legitimate company.
2. You are told that you need to update personal information for security purposes.
3. Concerned about safety, you click on the link those points to the counterfeit website.
4. You land on a website that looks exactly like the real one.
5. You enter your personal information and attempt to login.
6. The hacker now has your information – you've just been phished. You are at the mercy of the "phisher-man" or hacker. They can hijack your account; go on a spending spree, or selling your account information in the online black market.

As you can see, it only takes about a minute or less to get hacked. Fortunately, you can protect yourself. Follow these tips below.

How to Protect Yourself – 4 Simple Steps

1. Search for your name in the email. Most phishing attacks target a large group of people. As a result, the hackers don't really care about individualized information – they just want to hack as many accounts as possible. Thus, be cautious when you see something like "Dear Valued Customer."
2. Don't click the link. Instead of clicking the link, hovers the cursor over it. You will then see a pop-up notification of the link address. If the link reveals that the website is not from the actual company, don't click it.

3. Take a close look at the URL. If you clicked on a link, you can still determine if the site is a fake. Take a look at the Web address field on top of your screen. In most cases, secured login pages like social networks and online banks start with "https" in the address field. If you don't see it, do not sign in.
4. Search for grammatical errors. While hackers are good at stealing and divulging information, their syntactical and spelling skills are often subpar. Therefore, if the email is unprofessional and marred with grammatical errors, don't click the link.

5. Use anti-phishing software. These applications usually come with an Internet security suite. They detect phishing and websites and prevent you from divulging information.

Are You Just too Smart to Be Phished?

Some people may reason that they are too computer savvy or just too smart to be phished. Don't deceive yourself! Many big corporations have been faced with phishing attacks. You have no doubt seen and heard of successful hack attacks launched at social networking and even government sites.
One type of phishing attack that is particularly dangerous is spear phishing. Unlike most phishing attacks, spear phishing focuses on a specific person, company, group, or corporation. This means that the hacker can launch more precise attacks. For example, they can use your actual name instead of "Dear valued customer." Accept the fact that phishing is a serious threat and strive to follow the advice mentioned above to safeguard your information.