# What is Phishing?

Phishing is a cybercrime. It is received by email, phone, or text message from a cyber criminal pretending to be an organization/person that is legitimate. They lure you into giving up sensitive information such as passwords, bank/credit card information, or personally identifiable information. After they get this information, it's used to gain access to your accounts, putting you at risk of identity theft and financial loss.

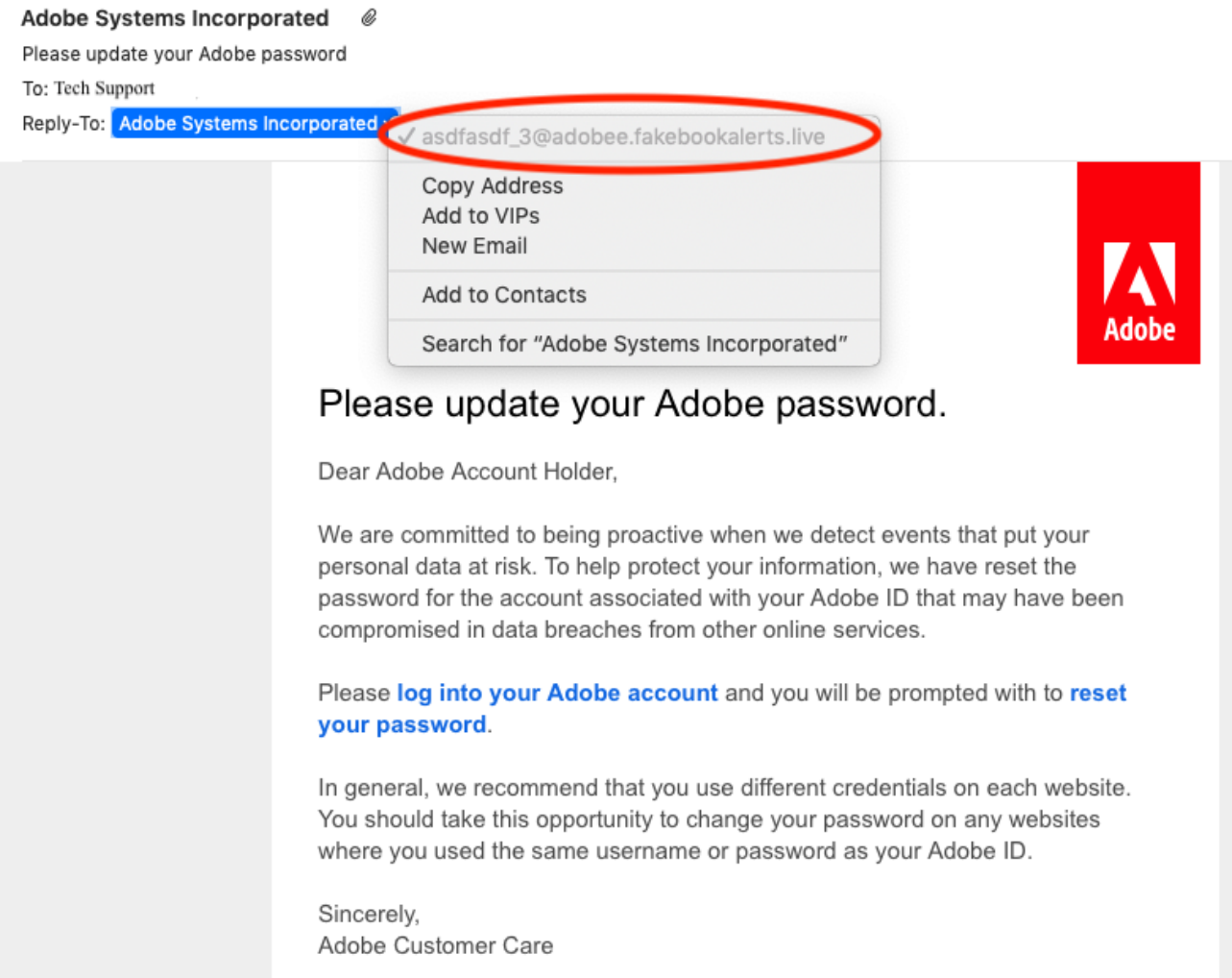
## Types of Phishing Attacks:

- **Social Engineering** - On your Facebook or LinkedIn profile, you can find: name, date of birth, location, workplace, interests, hobbies, skills, your relationship status, telephone number, email address and favorite food. This is everything a cybercriminal needs in order to fool you into thinking that the message or email is legitimate.
- **Link Manipulation** - Most methods of phishing use some form of deception designed to make a link in an email appear to belong to a legitimate organization or person. Misspelled website addresses are common tricks used by phishers. Many email clients and web browsers will show a preview of the links destination in the bottom left corner of the window while hovering the mouse cursor over a link.
- **Spear phishing** - Phishing attempts directed at specific individuals or companies have been termed Spear Phishing. Attackers may gather personal information (social engineering) about their targets to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.
- **Clone phishing** - A type of phishing attack whereby a legitimate, previously delivered email containing an attachment or link has had its content and recipient address(es) swiped and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version, then sent from an email address that is spoofed to appear to come from the original sender.

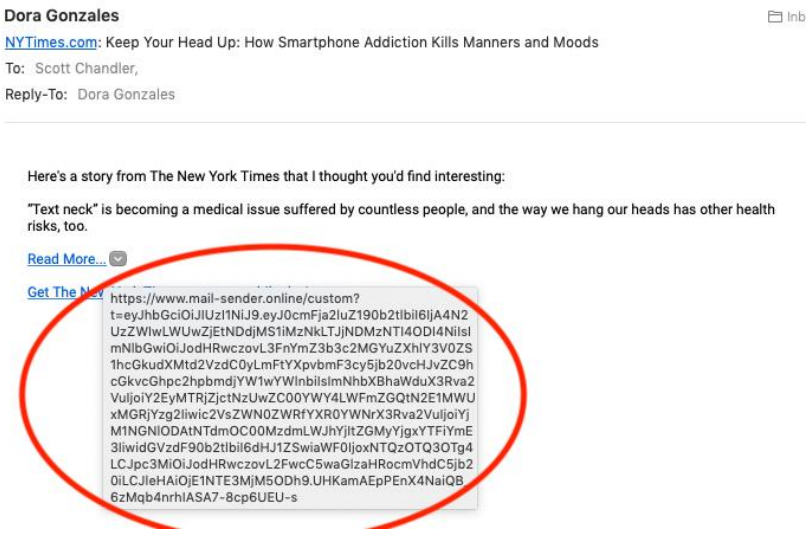
### What to do if you think you have received a phishing email.

- DO NOT click on any links within the email or download any attachments.
- If you recognize the sender but aren't expecting an email with attachments or links please contact them directly and ask if they had sent the email to you.
- If you are unsure if the email is legitimate or not, please contact help desk for assistance.

### Examples and tips to identify phish attacks




1. Looking at the sender's email address, you can see that this is not from a valid adobe email address, but rather a "fakebookalerts.live" address. This should be the first warning that this is **not** a legitimate email since it's talking about an adobe password change. Also if you look closely in this example the subdomain is "adobee" instead of "adobe"




2. In this example, this link is not a part of the New York Times domain, but an external site at mail-sender.online. This should be another warning that this is not a legitimate email.

*Sources:*

http://www.phishing.org/what-is-phishing
https://www.valdosta.edu/