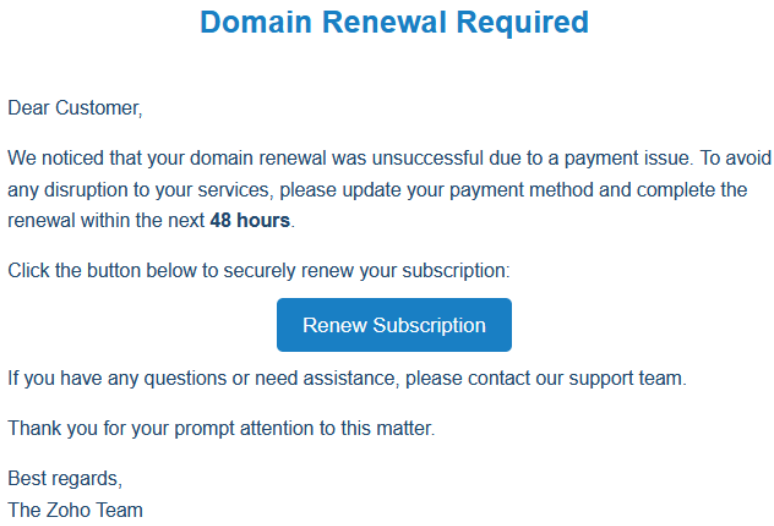
Anatomy of a Spear Fishing Attack

The webmaster for a site, https://www.ccc-cafe.com/ received this message recently. Subject line reads"***Domain Suspension Imminent – Update Required***".



Domain Renewal Required

Dear Customer,

We noticed that your domain renewal was unsuccessful due to a payment issue. To avoid any disruption to your services, please update your payment method and complete the renewal within the next **48 hours**.

Click the button below to securely renew your subscription:

Renew Subscription

If you have any questions or need assistance, please contact our support team.

Thank you for your prompt attention to this matter.

Best regards,
The Zoho Team

Just to be clear, the webmaster for the above site is also the author of this article.

The sender's email address was zoho@contact.com. Looks OK, but there is no contact.com listed anywhere. Pressing the blue *Renew Subscription* button would take us to http://****-****.yinyangfinance.** (slightly altered for safety), ostensibly in France but impossible to tell. Not to be too technical, but there is a very important distinction between **http and https**. The **"s"** indicates that the site has a security certificate. Now, yinyangfinace apparently does not have such a certificate. A little odd that a "finance" company would not be secure?

So, how did the webmaster of the site become a target of this attack? In web marketing, there are two schools of thought. First is to keep information out of sight, using forms for contact with prospects. This is designed to limit some spam type abuse. The second is to share as much contact information as possible, inviting prospects to get in touch easily and quickly. It also opens up the likelihood of receiving some unwanted spam. The strategy for the above site utilizes the second approach. So, it was not a challenge for the attacker(s) to get in touch. Forgive the pun, but there is a yin and a yang to both approaches. And the webmaster, being careful, had no trouble dealing with the threat. Basically, ignoring it defeats the attack.

OK, what makes this a *Spear Phishing* attack and not just a *Phishing* attack? One thing. The attacker(s) knew that the site utilizes Zoho for some purpose. Zoho is a company that provides many services and somehow the attackers knew of that relationship.

While these attacks are more ubiquitous than ever, they are easy to defeat when folks remain diligent. Basically, ignoring them and deleting the message is all we have to do. Never opening a suggested link in an email is the safest way to go. Communicating directly with the sender from the organization's web page is highly recommended.