**Phishing Tools and Techniques**

We have all had these type of messages at one time or another in our emails… “You have won a lottery” or “Win a Free Trip to Disney Land by entering this Lucky Draw”. The reality is far different than what these emails promise. Most of the times, these emails are phishing scams and clicking on the links redirect you to fake websites intending to “phish” your personal information.

Most of us are already familiar with the term “phishing”. It is an internet fraud in which the cybercriminal tricks an individual into providing their sensitive information. Phishing scams are usually intended to collect credit card numbers, account passwords, and social security numbers. These can be used to make false purchases. Other information such as name, date of birth or address can be used for committing identity thefts.

Phishing can take many forms and can be achieved with many tools and techniques. Here, we highlight the most common tools and techniques that are used to carry out phishing scams.

**Link Manipulation**

Link Manipulation is a widely used technique for phishing scams. It is done by directing a user through fraud to click a link to a fake website. Generally, many users are now aware that they do not need to click on links that may seem suspicious in first look. Hence, hackers are now using manipulative ways to get the users to click.

Let us look at some of the ways hackers use link manipulation to their advantage.

1. **Use of Sub-Domains:**

For nontechnical users who may not be familiar with sub-domains, this trick works like a magic for the hacker. Consider for example, you get an email from a renowned xyz bank that asks for your credentials and requests you to click on the url [www.xyzbank.user.com](https://securityiq.infosecinstitute.com/). A nontechnical person will consider that the link would direct to a “user” section of the xyz bank. In reality, the link takes you to the “xyzbank” section of the website [www.user.com](https://securityiq.infosecinstitute.com/). Though the domains are unique but sub-domains are not, and hence no domain owner can control anyone from using their name as a sub-domain of their domain. Whether technical or nontechnical, one should always remember that the URL hierarchy always goes from right to left. Hence a link that says mail.yahoo.com will take you to domain of yahoo with sub-domain as mail, whereas yahoo.mail.com will lead you to the domain mail.com with subdomain as yahoo.

1. **Hidden URLs:**

Another commonly used link manipulation technique is when a phisher hides the actual URL under plain text. This means that rather than displaying the actual URL, they use sentences such as “[Click Here](https://securityiq.infosecinstitute.com/)” or “[Subscribe](https://securityiq.infosecinstitute.com/)”. In reality, the URL hiding behind the text leads you to phishing websites. A more convincing email could even display the actual link, such as [www.americanexpress.com](https://securityiq.infosecinstitute.com/), but if you click the link it would lead you to an unexpected website. Another method of hiding the URL is by using shortening tool such as tinyurl or bit.ly. (You don’t need to worry about clicking these links, as all of them take you to Security IQ’s Phish Sim tool portal).

With increased number of users on social media networks, phishers are able to cast wider nets with greater opportunities to succeed. With social media, the trust factor for which phishers otherwise work very hard is already there. People follow and receive messages from other people and services they trust. Skeptical users may easily spot rogue messages, but most of the time these go undetected and tempt users for clicking. With only one malicious link, a hacker can easily target many users in one go. Since URL shorteners are extensively used on social media, it is hard to tell in advance where the link will actually take us.

To avoid clicking a manipulative hidden URL, always hover your cursor over the link and check to see the actual link where the URL is directing you to. In case the link seems “phishy”, do not click it.

1. **Misspelled URLs:**

Another common link manipulation technique is when a hacker will buy domains with a variation in spellings of a popular domain, for example, facebok.com, googlle.com, yahooo.com, etc. They then fool the users by making similar looking websites and asking for personal information. This technique is also known as URL hijacking or typosquatting. The advantage it gives to a malicious user is that they don’t even need to be sent via email to be accessed. Rather, a little carelessness in typing can lead many users to them.

1. **IDN Homograph Attacks:**

In this technique, a malicious individual misguides a user towards a link by taking advantage of similar looking characters. For example, a user who frequently visits Citibank.com may be directed to click a link in which latin C is replaced by Cyrillic C. Moreover so, characters that seem similar may also be used to deceive. For example, capital of i (I) and small L (l), both look the same. Similarly, zero (0) and capital o (O) also look the same when typed.

**Website Forgery**

Website Forgery is another phishing technique that works by making a malicious website impersonate an authentic one, so as to make the visitors give up their sensitive information like account details, passwords, credit card numbers, etc.

Web forgery is mainly carried out in two ways i.e. Cross-Site Scripting and Website Spoofing.

1. **Cross-Site Scripting**

Cross-Site Scripting or XSS refers to an attack where a hacker executes malicious script or payload into a legitimate web application or website. It is a very common and most widely used technique in which the victim is not directly targeted. Rather, the attacker exploits a vulnerability in a web application or website that is visited by a user. Eventually, a malicious script is delivered to the victim’s browser.

Though hackers can take advantage of XSS within ActiveX or VBScript also, but the most commonly abused is JavaScript, primarily because it is used by nearly all websites of today.

**In order to make it work**, an attacker will need to inject a payload into a page visited by the victim. To make you visit a page, the attacker has to use social engineering or link manipulation techniques. To make it further successful for the attacker, the user then needs to input their data directly into the fake website’s pages. After this, the attacker will insert a string to be used in the webpage and treated by the user’s browser as code. When the browser loads the page, the malicious script executes without the victim even knowing that such an attack has taken place.

**Protection against XSS is possible**, though it may not be totally avoidable. Some browsers come with built-in XSS protection, so it is always a good practice to check your browser’s security options and update the browsers to the latest versions. Some add-ins like NoScript for Firefox let you allow or deny permission. NoScript also lets users reject websites other than the ones chosen by them for their usage.

1. **Website Spoofing**

Another technique used for web forgery, website spoofing, is done by creating a fake website that looks similar to a legitimate website which the user actually intends to access. A spoof website has a similar user interface and design and often has a similar URL. If you are in a hurry and not paying much attention, you can easily fall prey to such sites that appear identical to their legitimate versions. If you have not manually typed a URL and are landing on a webpage by clicking a certain link, you need to be particularly skeptical about it. As already discussed in our Link Manipulation section, always look out for the possibility of URL cloaking. To be sure, hover your cursor over the link to check the actual URL where the link is taking you to.

**Pop-Ups:**

Pop-up messages are one of the easiest techniques to conduct successful phishing scams. These allow hackers to steal login details of users by sending them pop-up messages and eventually leading them to forged websites through these pop-ups.

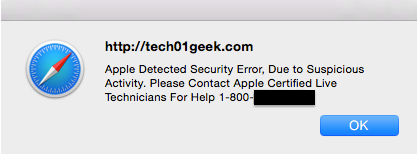
A variant of phishing attacks, also known as “in-session phishing”, works by displaying a pop-up window during an online banking session and appears to be a message from the bank.

A typical “in-session phishing” scenario would look like this:

* You log into your online banking account
* You may leave your browser open and check another website in another window
* A pop appears after some time, supposedly from your bank, and asks you to retype your username and password as your previous session has expired.
* You enter your details, least expecting the popup to be a fraud, since you had already logged into the bank’s website.

Another recently widespread pop-up phishing scam is the “popup tech support”. When browsing the internet, you will suddenly receive a pop-up message that your system is infected and you need to contact your vendor for technical support.

An example of this is shown below:

****

**To avoid this**, try not to respond to popup windows that appear spontaneously without your clicking a hyperlink. Moreover, block popups in your browser settings and always log out of your banking sessions and other sensitive accounts soon after your work is complete.

***Security IQ’s PhishSim Tool*** provides many templates that can help accustom its users with real world phishing techniques such as link manipulation and web forgery.

An example from the PhishSim tool below displays Link Manipulation through hidden URL technique.

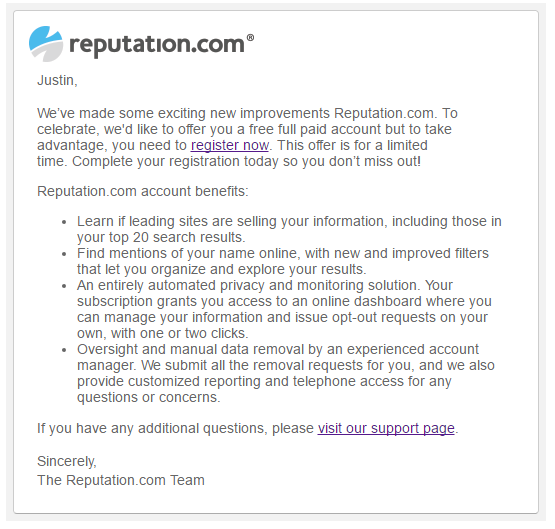


Figure below shows a template from our Phish Sim Tool. If a user clicks on the “Confirm Friend” tab, it will take him/her to a spoof website.

