The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Understanding URLs
- URL Shorteners
- QR Codes

URL Shorteners / QR Codes

Background

A Uniform Resource Locator (or URL) is nothing more than a fancy term for a website address, such as http://www.google.com. A URL is the name you type when you want to visit a website or web page. When you type a URL into your browser, your browser takes the name and resolves it into an IP address; that IP address is where the website is located on the Internet. Your browser then connects to the website and downloads the page to your browser, which you then view. The problem is cyber criminals can play a variety of tricks on you with URLs, making you think you are visiting a legitimate site when you are really visiting a different website controlled by them: one that is most likely designed to steal your information or attack your browser and infect your computer. Where you think you are going and where you are actually going can be two different things. Let's review how a URL works, several common URL attacks and how you can protect yourself against them.

Guest Editor

Dr. Eric Cole is an industry-recognized security expert. He is the author of several books, including Advanced Persistent Threat, Hackers Beware and Network Security Bible. Dr. Cole is also the founder of Secure Anchor Consulting and a SANS faculty Fellow and course author.

Understanding URLs

A URL is nothing more than a destination made up of three parts. The first part is the protocol, or how you are connecting to the website. This is normally HTTP (clear text) or HTTPS (encrypted connection). The second part is the domain, which is the website you are going to. The third part is the landing page, or the page you will visit on the website. Let's look at a sample URL:

https://www.securingthehuman.org/ouch

This URL begins with HTTPS, which indicates it is an encrypted connection. The second part, www.securingthehuman.org, is the website that you would visit if you were to click on the link. Finally, the third part is the '/.' Anything after the forward slash indicates what part of the website you would visit. In this example, you would be going to the Securing the Human website, and then be directed to the

© The SANS Institute 2013

URL Shorteners / QR Codes

latest OUCH! pages. The most important part to examine is the second part -- the domain. Is that really the website you intend on visiting? Let's see how bad guys can play tricks on you and send you to websites that they control.

To be safe, first verify the true destination of shortened URLs or QR codes before clicking on them.

URL Shortener

You most likely have seen a URL shortener before; it is nothing more than a service that takes very long, complex URLs and shortens them to very short, simple URLs. This makes it easier to communicate long or complex URLs through traditional communications, such as in email. It is also used when the number of characters is limited, such as on Twitter or text messaging. Examples of such shortening services include tinyurl.com, bit.ly or goo.gl. The risk with these is that when you click on a shortened URL, you can't see the true destination. As such, attackers can post shortened URLs that ultimately take you to websites they control.

One of the ways you can protect yourself is to verify where a shortened link will take you before you click on the link. Several websites offer a service that lets you copy/paste a shortened URL and see its true destination (see Resources for examples). In addition, some URL shorteners give you the option of previewing the true destination. For example, if you have a bit.ly URL, simply add a '+' to the end of the URL to see the true destination, like this:

http://bit.ly/10hVtvV+

QR Codes

A QR code is similar to the concept of URL shorteners, but designed for your smartphone. It converts a URL into a digital image. By using a special app on your mobile device, you can take a picture of the QR code, which then opens a browser on your mobile device and takes you to the website embedded in the QR code. However, you run the same risk associated with URL shorteners, in that you are trusting the QR code and you do not know where it is going. For example, let's say you are at a train station or

© The SANS Institute 2013

URL Shorteners / QR Codes

airport terminal and you see a poster advertising a new movie. If you use your smartphone to read the QR code, the poster promises to take you to a movie trailer. While the poster is most likely legitimate, any criminal could have easily walked up to the poster and pasted a new sticker with a QR code they've created over the existing one. Now any device that were to read the QR code would be redirected not to the movie trailer, but to a website controlled by the attacker.

Just like with a URL shortener, first verify the destination. Be sure your QR code reader app supports the ability to show you where it is taking you, then gives you the option of deciding if you want to visit the website or not. If your QR code reader app does not give you the ability to preview the destination, get a new one, as there are many free options.

Special Purchase Program

Are you employed in Education or State & Local Government? Do you need security awareness training but have a limited budget? If so, now is the time to take advantage of a limited time offer through the SANS Institute. Now through July 31st, receive discounts on Securing the Human for End Users & Developers, OnDemand Courses, GIAC certifications, and NetWars Continuous. For more information, please visit:

- Educational Institutions – http://www.sans.org/renisac
- State & Local Governments – http://www.sans.org/cis

Resources

Explanation of QR codes:	http://en.wikipedia.org/wiki/QR_code
Unfurlur:	http://unfurlr.com/
URL X-ray:	http://urlxray.com/
Common Security Terms:	http://www.securingthehuman.org/resources/security-terms
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

OUCH! is published by SANS Securing The Human and is distributed under the Creative Commons BY-NC-ND 3.0 license.
You are free to distribute this newsletter or use it in your awareness program as long as you do not modify the newsletter.
For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis