OUCH! | August 2012

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE…

Counterfeit Websites

GUEST EDITOR

Arrigo Triulzi is the guest editor for this issue. He is a certified SANS instructor and an independent security consultant working out of Geneva, Switzerland.

OVERVIEW

One of the advantages of shopping online is the ability to find the product or service you want, but at lower prices. Criminals know this and will take advantage of your desire to find an online bargain. Criminals will create fake websites that appear legitimate, but will sell you counterfeit goods or even worse, simply not deliver anything at all. In this newsletter we give an example of such an attack and then explain how you can protect yourself from similar fraud.

EXAMPLE OF A COUNTERFEIT WEBSITE

Let's pretend you need to purchase a baby carrier, perhaps as a gift for a friend who has a newborn. You decide to look for a bargain online and begin with a search for baby carriers, specifically BRAND X baby carriers as you know that is what your friend prefers. You quickly discover that multiple sites sell the same baby carrier, however the prices vary greatly. You select the website that has the cheapest prices and purchase the product online. Several weeks later you receive the product, only to discover it does not look quite right – some of the pieces are wrong, the material is defective, or the product is outdated. You attempt to call the website to return the product only to discover there is no phone number. You then e-mail the website but never receive a response to any of your complaints. You just purchased a counterfeit (or stolen) product from a counterfeit website.

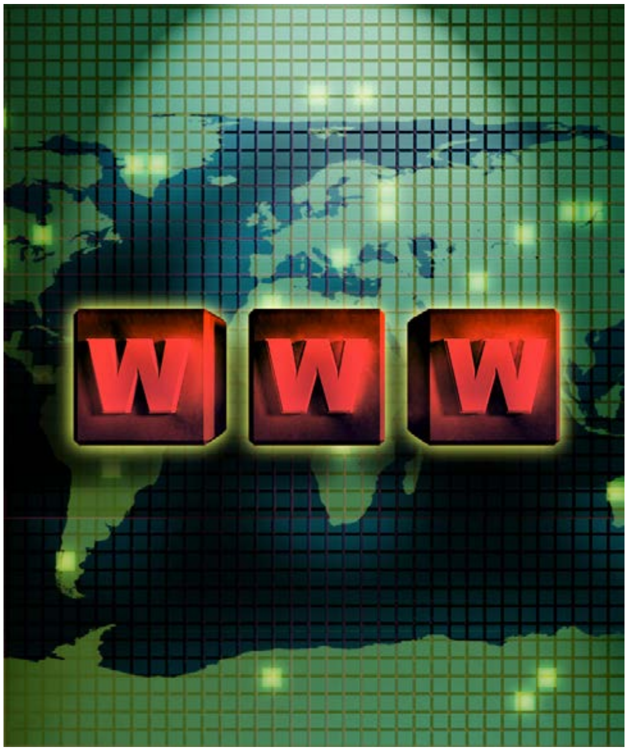
What happened is that criminals simply copied the legitimate website of the original manufacturer (in this case BRAND X baby carrier), posted this website under a new domain name that they control, and then significantly lowered the prices to encourage people to buy from this rogue website. The items they deliver to you are counterfeit, stolen, or used products, or they simply do not send anything at all. As such, whatever they charge is pure profit for them.

Counterfeit Websites

PROTECTING YOURSELF

We understand that you want to leverage the Internet for the best possible shopping experience.   Here are several steps you can take to protect yourself from attacks like these.

1. If the pricing seems to be good to be true, be very suspicious.
2. Call their support number. Wait ... no support number or contact listed to call? Another red flag.
3. Often the criminals that set up these counterfeit websites are not native speakers of the website's language. The e-mails they send you may have poor grammar or simple spelling mistakes. In the case of one counterfeit baby carrier website, one of their e-mails opened with, "*We wish to welcome you to BRAND X baby carrier, Cheap baby carrier BRAND X, on sale,Free shipping*." Respectable businesses have their e-mails proofread before sending them to real customers. When you see poor grammar or spelling, be very suspicious.
4. Criminals will often use the brand name of the goods you are searching for in the URL so they look legitimate to you. But they also frequently change the URLs of their counterfeit websites, making it harder to shut them down. As a result, criminals will often use several different domain names and e-mail addresses during the purchasing process. For example, in our example of the baby carrier website, the cyber criminals may have one domain name for the website (such as www.brandxbabycarriers.com), another domain name for the e-mails they send you (such as from sales@brandxcarrierstogo.com), and a third domain name for support e-mails (such as support@babycarriersbrandx.com). All these different domains are another big red flag.
5. Legitimate organizations should always use encryption during the online purchasing process. If encryption is not used for the online transaction, then do not buy from the website. You can



If a website is selling products or services at a price too good to be true, be suspicious, the website may be a fake.

determine if the website is using encryption if the URL has HTTPS and your browser is showing the padlock.

6. Do a search on the name or URL of the online store and see if anyone else has posted any complaints about the website indicating fraud. For example, if you are purchasing items from www.brandxbabycarrier.com, do a search on that URL first and see if others are complaining about fraudulent goods.
7. Use PayPal or other mechanisms that do not reveal your underlying credit card information to the merchant. For example some credit card providers will give you one-time use credit-card numbers. Another option is to use gift cards.
8. Consider using security software that helps rate the trust level of websites you visit.
9. If you are concerned that you cannot tell if a site is legitimate or not, then do not use the site. Purchase the product from a well known site you trust instead. You may not get the best deal, but you will be able to trust the product and the return policy.
10. If you do fall victim to online fraud, report it to the Federal Trade Communication or the law enforcement agency of your country. In addition, call your credit card provider and cancel your existing credit card to protect yourself from any further online fraud, and ask them to issue you a new one.

RESOURCES

Some of the links have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

Web of Trust:
http://www.mywot.com/

SiteAdvisor:
https://www.siteadvisor.com/

Reporting Complaints to FTC:
https://www.ftccomplaintassistant.gov/

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org