HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

WEEKLY

Volume #4 - Issue #168
July 13th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Web Spoofing

Are you certain that the site you are looking at is what it appears to be? Does the website really belong to the company or bank that you think you are doing business with?

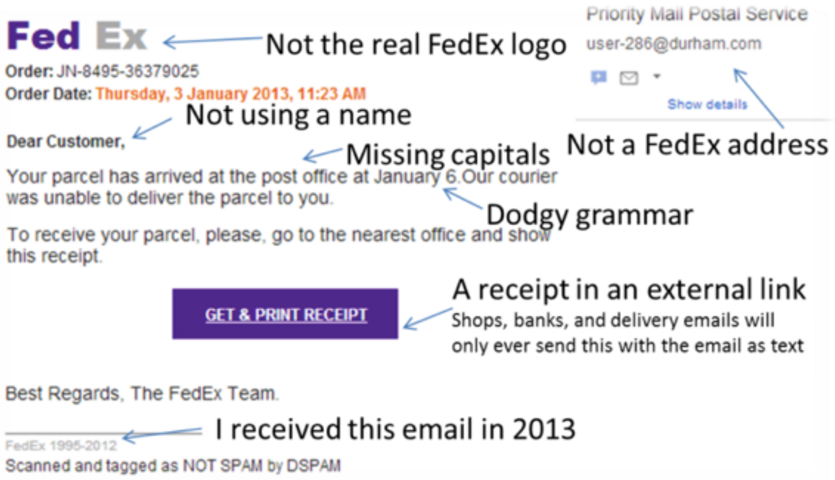
This is how website spoofing happens: You click a link on a page or in an email you have received because the email looks like it is from your bank, it has their familiar logo and all their usual wording in it. The clicked link takes you to a page with the usual account login fields for you to put in you username and password. The URL up in the address bar is the usual URL for your on-line banking and so you're pretty comfortable. You type in your username and password but for some reason it doesn't take. You try again and you're logged in in the usual fashion and see all your account details. Everything is as it should be. Or is it? Unfortunately, it is very possible that you have just become a victim of a crime involving a "spoofed" website address and the contents of all your bank accounts are now at risk. How does it work, and what can you do to protect yourself? Here is how this can happen to you without your knowledge.

The hacker starts by obtaining a legitimate email from the bank in question. This could have come from an actual account they, or one of their associates opened, or it may have come from the email program in a lost or stolen notebook or home computer. They also copy the login page from the bank. Using phony ID they set up a site on a hosting company somewhere and put up the copy of the login page, but with some code written into it to capture the entered username and password and transfer the visitor to the legitimate login page.

Next, they send out the emails with some pretext that requires you to login and check something on your account. The emails have spoofed (copied) sender and return addresses so that they look like they came from the bank. The link in the email uses another spoofing technique to display the legitimate website address in the address bar and status bar of your browser while actually displaying the fake page. You click it, it takes you to the fake page, but everything looks normal to you. You type in your username and password; the fake page captures your identification and sends you over to the legitimate login page. Depending on the way the bank's site (or auction, or web payment or any other financially useful page) is constructed, it might also be possible for the fake page to pass your identification over to it so that it logs you right in without you having to type it a second time. So all your financial, or other information that you use on that particular site, has been stolen, and you have no idea it just happened.

So how do you prevent this? (Because prevention is so much better than cure!) The best way to prevent yourself from becoming a victim of a spoofed site is to never use a hyperlink to get to a financial page unless you are CERTAIN that it is a legitimate link. That means, never use a link in any email to take you to a financial page. Instead, type the address into the address bar yourself. This is a minor inconvenience compared to having your bank accounts emptied. If you started by typing in a known address to a site and you are now following links through the site to its secured financial pages, you can be pretty sure they are legitimate links. If you've been taken off to another site somehow, and are now being returned to the financial pages, I'd be more cautious if I were you, look at the URL address at the top of the page and make sure it has a "https" prefix. (As opposed to just a "http" prefix.) If you typed in the address to a site to visit it and then saved it in your "favorites" Bookmarks, you can generally trust it (unless you believe somebody with malicious intent might have had access to your favorites list). The best way, however, is to memorize the address and type it in yourself.

Examples of Common Web Spoofing Scams:



Priority Mail Postal Service
user-286@durham.com

Order: JN-8495-36379025
Order Date: Thursday, 3 January 2013, 11:23 AM

Dear Customer,

Your parcel has arrived at the post office at January 6.Our courier was unable to deliver the parcel to you.

To receive your parcel, please, go to the nearest office and show this receipt.

Best Regards, The FedEx Team.

FedEx 1995-2012
Scanned and tagged as NOT SPAM by DSPAM

Not the real FedEx logo

Not a FedEx address

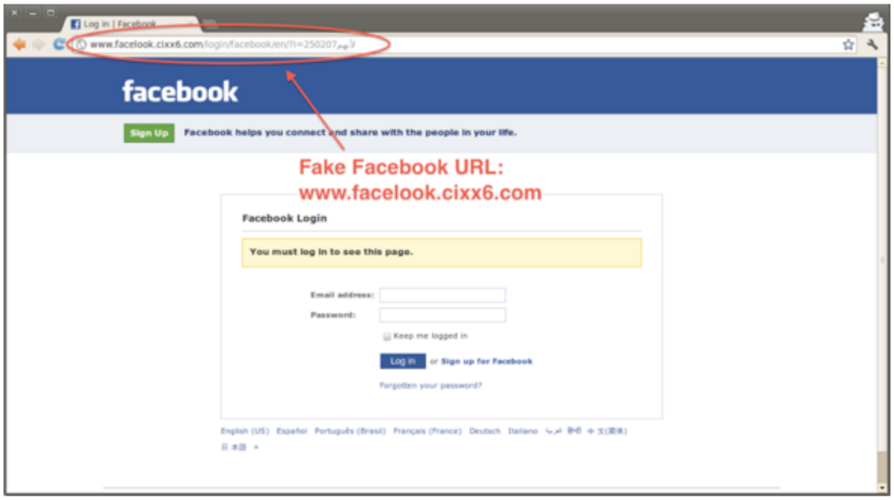
Not using a name

Missing capitals

Dodgy grammar

A receipt in an external link
Shops, banks, and delivery emails will only ever send this with the email as text

I received this email in 2013



Log in | Facebook
www.facelook.cixx6.com/login/facebook/en/?i=250207
facebook
Sign Up

Facebook helps you connect and share with the people in your life.

Fake Facebook URL:
www.facelook.cixx6.com

Facebook Login

You must log in to see this page.

Email address:

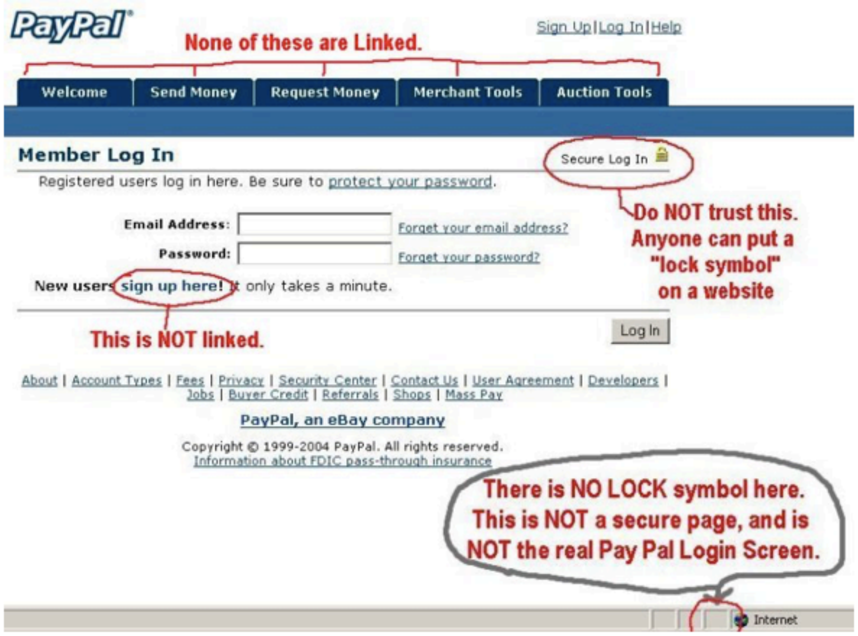
Password:

□ Keep me logged in

Log in or Sign up for Facebook

Forgotten your password?

English (US) Español Português (Brasil) Français (France) Deutsch Italiano



None of these are Linked.

Member Log In

Secure Log In

Registered users log in here. Be sure to protect your password.

Do NOT trust this. Anyone can put a "lock symbol" on a website

Email Address: Forget your email address?

Password: Forget your password?

New users sign up here! It only takes a minute.

This is NOT linked.

About | Account Types | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs | Buyer Credit | Referrals | Shops | Mass Pay

PayPal, an eBay company

Copyright © 1999-2004 PayPal. All rights reserved.
Information about FDIC pass-through insurance

There is NO LOCK symbol here. This is NOT a secure page, and is NOT the real Pay Pal Login Screen.

Thank you for subscribing to our email!

Home Cyber Defense Weekly

is a service of

House of File Technologies