Check what URL is actually used when using banks or submitting credit card information! The number of Phishing scams is increasing.

Check what URL is actually used when using banks or submitting credit card information! The number of Phishing scams is increasing.

2004-08-16, LinuxReviews.org

Phishing means setting up a website that looks exactly like a known trusted service in order to lure you into submitting credit cards, pin-codes or other valuable information. You may think you are using a bank, financial institution or web-shop when you are actually submitting information to a fake phishing site.

Netcraft reports the Life Span of a Phishing Site Averages 54 Hours and the number of fraud attempts is increasing.

They are also becoming more sophisticated, as the fake Paypal Customer Service scam attempt reported by the Anti Phishing Work Group on 2004-08-13.

A mass mail looking like a normal PayPal message was mass-mailed. It begins Dear PayPal valued member, and looks authentic enough to be accepted as real. It explains that you need to renew your account and asks you to Please follow the link below and renew your account information.

Some mail readers will show the link as https://www.paypal.com/cgi-bin/webscr?cmd=login-run.

The actual code making the link is

Check what URL is actually used when using banks or submitting credit card information! The number of Phishing scams is increasing.
The link will take you to www.paypal.mfrt.net, not www.paypal.com like it may appear.

**The thief's move fast and work globally.** APWG documented one scam that operated a fake website using seven different servers over a period two weeks, using four servers in Korea, one in Uruguay, and two in the US. The life-span of a website at a single web-server is 54 hours, less than three days. The website where you accidentally gave away your credit card number is long gone without a trace by the time you notice those unfortunate huge bills.

The number of scams increased by 52 percent from May to June. Nearly to 500 of the 1,422 attacks in June targeted Citibank alone. Other popular targets include eBay, AOL, US, Bank, MSN, Fleet, Bank, Wells Fargo and VISA.

**Remember, use the latest available version of your favorite browser!** Opera versions <=7.52 can be fooled into showing a faked URL in the address bar! The problem is fixed in Opera version 7.54. Some versions of Internet Explorer has a similar problem. Mozilla and Mozilla Firefox still has a open bug that allows carefully crafted websites to draw a fake location bar above the real one...

Always check what URL you are visiting, and do take a look at SSL certificates before you accept them.

Check what URL is actually used when using banks or submitting credit card information! The number of Phishing scams is increasing.
The following, by chance, fell down in my in-box hours after this was originally posted...:

From: PayPal Support <paypal@paypal.com>

Dear valued PayPal member:
<br>It has come to our attention that your PayPal billing updates are out of order. If you could please take 5-10 minutes out of your online experience and update your billing records you will not run into any future problems with the online service. However, failure to update your records will result in account termination. Please update your records.
<br>Once you have updated your account records your PayPal session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.
<br>To update your PayPal records click here:
<br>
<br>PayPal Customer Service
<br>http://www.PayPal.com

> Linux Reviews > News and headlines > 2004 News archive > August > Check what URL is actually used when using banks or submitting credit card information! The number of Phishing scams is increasing.