

Criminal Websites: Phishers
By Frank, *Your Computer Tutor*

It is very easy for a person with evil intentions to clone a real website or to virus-infect your computer to make it a host for a criminal website - it costs them nothing but a little time to do this.

These criminal websites come in many forms: they are called Phishers. Phishers 1) try to steal your identity, 2) maintain fraudulent online shops, 3) provide tempting content that contain viruses or spyware, and 4) contain illegal or pirated content, and/or 5) promote worthless investments or get-rich-quick schemes.

“Phishing” is a scam; it starts by criminals sending email to thousands of unsuspecting folks, like you! These emails pretend to come from trusted organizations, banks, credit card companies, online shops and auction sites. These email messages usually contain compelling (but bogus) reasons to click on an embedded link in the email.

Clicking on the link takes you to a criminal website that looks exactly like the real thing – like your bank or credit card, but, it’s a fake. In fact, it’s really a site resembling (mirroring) the original site, designed to trick you into entering your personal information such as a password or credit card number.

These fake emails usually have the following characteristics: A call for a sense of urgency - “act immediately your account may be closed”; a request for your user name, password or banking details.

Here are some other clues that might give away a fake: There should be a physical address, a phone number or an email contact. Send an email or phone them to establish whether they really exist.

The website’s address may be different from, or perhaps there are extra characters or numbers and words in the web address. Right-click on the hyperlink, and selecting “Properties” reveals a link’s true destination and extension. Look for .com . net .org

www.beyondtechnology.net would be a legit site
www.beyondtechnology.80111.cz would be bogus

Remember, when you are on the internet, you are logged onto the World Wide Web (www) and many bogus sites are overseas, disguised as legit ones. Look for extensions from countries like: Bermuda (bm) Czech Republic (cz) Namibia (na) Russia (ru) A Colorado bank would have a .com, not an .ru extension You can find country extensions at <http://www.domainit.com/domains/country-domains.mhtml>

In the browser window, look for the padlock or ‘HTTPS://’ at the beginning of the web address. HTTPS signifies you are it is using a secure link.

Never judge a website by its appearance. It is easy to create flashy, professional-looking sites and it is easy to steal other people's web page designs and \$\$\$. Be wary of sites that are advertised in unsolicited emails from strangers – those that promise easy profits and avoid sites hyping investments, stocks or gold shares. Some schemes involve receiving money for other people and payments in advance.

Finally, you can find the status of a suspicious site by going to Alexa.com and entering the site address there, and "Google search" to see if anyone has had any problems with a suspicious-looking website.

Be Cautious and Happy Computing!!

MENTOR FRANK HARE, M.A., manages Colorado-based BeyondTech, LCC: IN-HOME SERVICES Offered:
Repairs – Networking - Spyware & Virus Removal - 24/7 – Powerful Custom-Built Computers & Tutoring
Hundreds of Happy Clients 303-575-1774 frank@beyondtechnology.net