Немного про фишинг

Оригинал запостил в juick: http://juick.com/hatred/498774

интересный вариант фишинга наблюдал буквально на днях. Да я являюсь обладателем пустого аккаунта на одноглазиках, в моем круге и мире, а так же вконтакте. Пользуюсь 99.99% последним, остальные - исторически сложилось. Про быдло не нужно, каждый считает что быдло кто угодно, только не он. Скучно.

Так, вот, многие помнят как шумели истории, когда «рыбаки» выуживали пароли хомячков, а те даже не замечали, пока от их имени активно не начинали спамить.

Делается обычно как: приходит письмо-подделка, полностью дублирующее внешний служебных писем (вашу фото прокомментили, кто-то просится к вам в друзья, на ваш счет поступил перевод и т.д. и т.п.) и ссылкой для быстрого перехода, причем домен там чуть-чуть, одной двумя буквами отличается от оригинала (нужно было озадачиться - коллекцию собрать, но да ладно), пример

- http://vkontakte.ru/mail.php (правильная ссылка)
- http://vkontakkte.ru/mail.php
- http://vkontate.ru/mail.php
- http://vkonttakte.ru/mail.php

и т.п.

По такой неправильной ссылке открывается сайт-подделка, при этом не сам сайт, а только диалог входа - ввод логина и пароля. И вот вы, счастливые, что к вам в друзья стучится Наоми Кембел, потными ручками вводите свой логин и пароль и... и он улетает в базу злоумышленникам, а они вас тупо перенаправляют на оригинальный сайт, где вас или повторно попросят ввести пароль или произойдет автовход.

Что в таких случаях делать? Прежде всего - ДУМАТЬ и быть внимательными, желательно регулярно менять пароли, если забываете, запаситесь на паре флешек синхронной копией базы и программы KeePassX (можно прочитать и как KeepAss... что часто больше отражает её суть), и храните пароли в ней, не ходить по ссылкам из письма, а набирать сайт вручную - нужные ссылки у вас и так скорее всего в истории сохранены (если параноик и чистишь постоянно, то это не про тебя)

Так, что-то лирика большая, собственно про сам вариант: в аккаунте у пользователя (форум, стучится новый контакт в ICQ/Jabber/etc) в качестве сайта указан хомяк на какой нить соц-сети, ессесно, интересно глянуть - а что такое, быстро копируешь вставляешь... и получаешь, что выше описано, причем инертность, по крайней мере у меня тут большая, но если появляется диалог входа, я таки внимательно изучаю ссылку. В этом варианте даже не надо заморачиваться на подделке письма, адресов обратных, а внешний вид страницы сайта, сдергивается httrack'ом, wget или curl'ом за пару секунд и дальше чуть чуть быдло-кодинга на чих-пых и готово. Так что будьте внимательны, мы тут на войне.

Хау. Я все сказал.

PS не только соцсетей это касается, просто пока они модны, и там тусуется в т.ч. много лемингов, они - лакомый кусочек, для спамеров в том числе. А так этом может быть какой нить интернет-банк, ещё что нить.