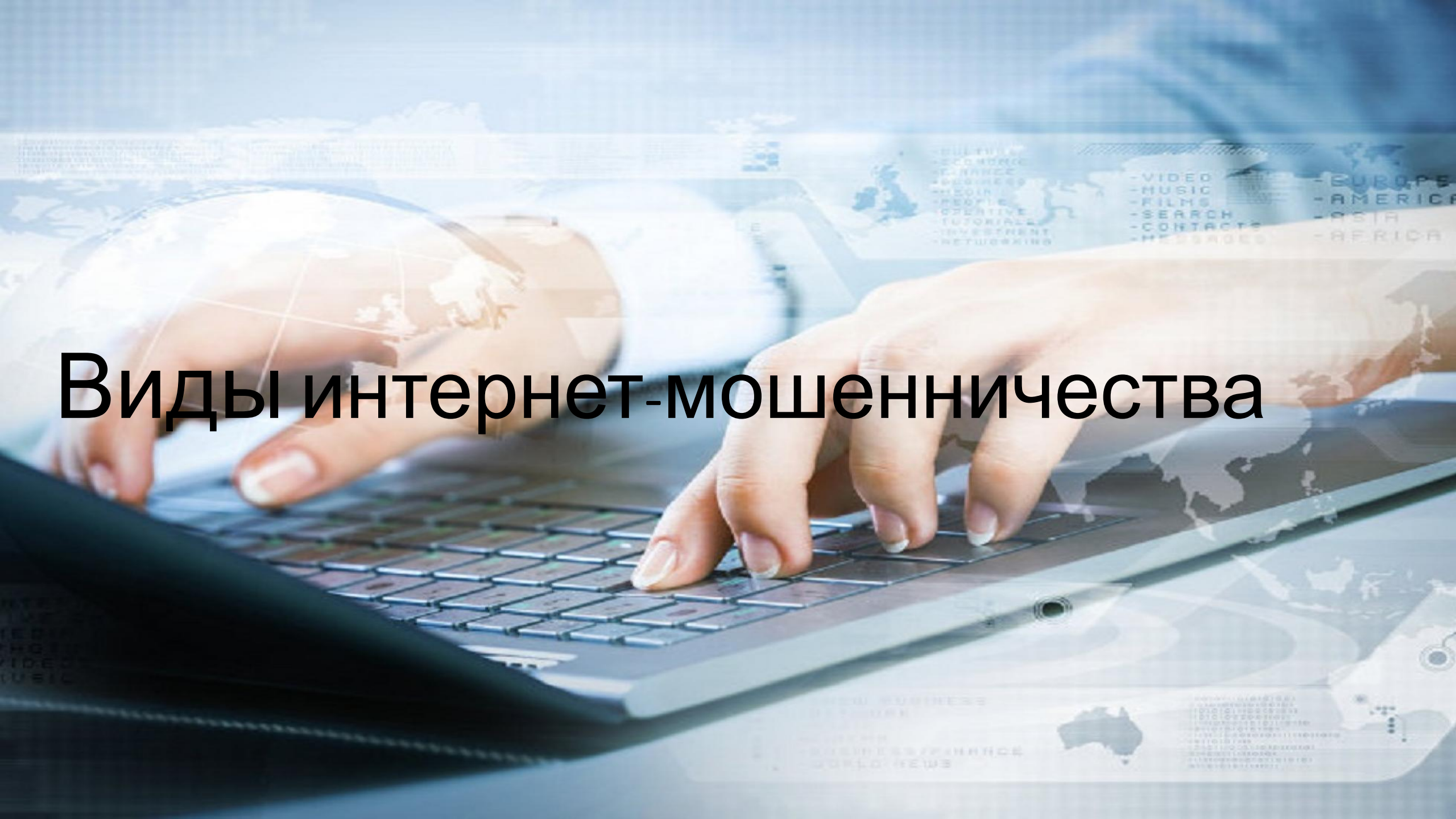
Мошенничество в Интернете



Виды интернет-мошенничества

1

Сообщение-Ваша банковская карта заблокирована

Что делать?

Для граждан: не сообщать реквизиты карты никому. Представители банка их знают! Ни одна организация, включая банк, не вправе требовать ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка.

При подключении дистанционного обслуживания в банке и пароля для Личного кабинета нужно выяснить, как именно он работает! В дальнейшем никому не сообщать разовые СМС-пароли подтверждения входа в Личный кабинет!

Основные схемы телефонного мошенничества

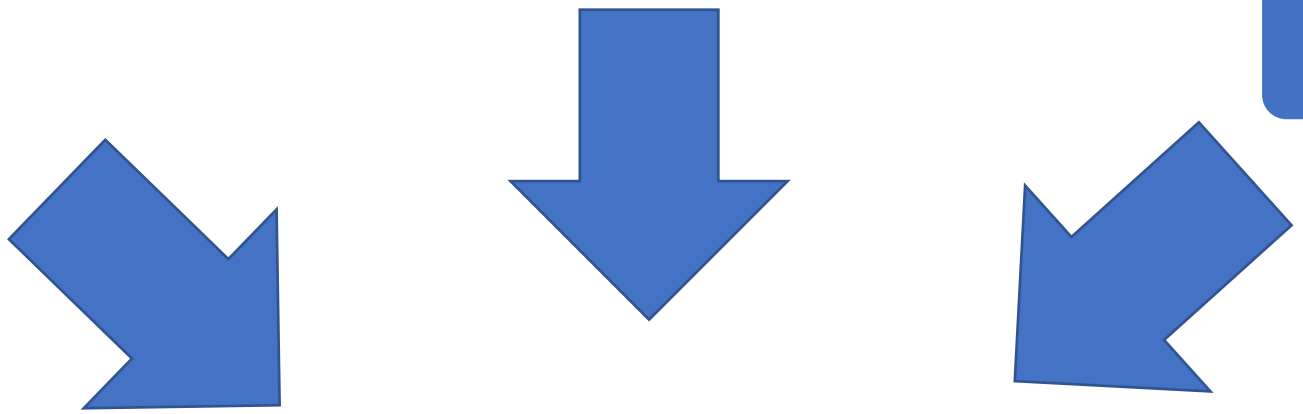
Обман : Родственник попал в беду , требование выкупа

Телефонный номер-грабитель

SMS-просьба о помощи

Выигрыш в лотерее

Телефонный вирус



Следует помнить что незнакомцем в интернете и в жизни не стоит доверять!!!

Фишинг

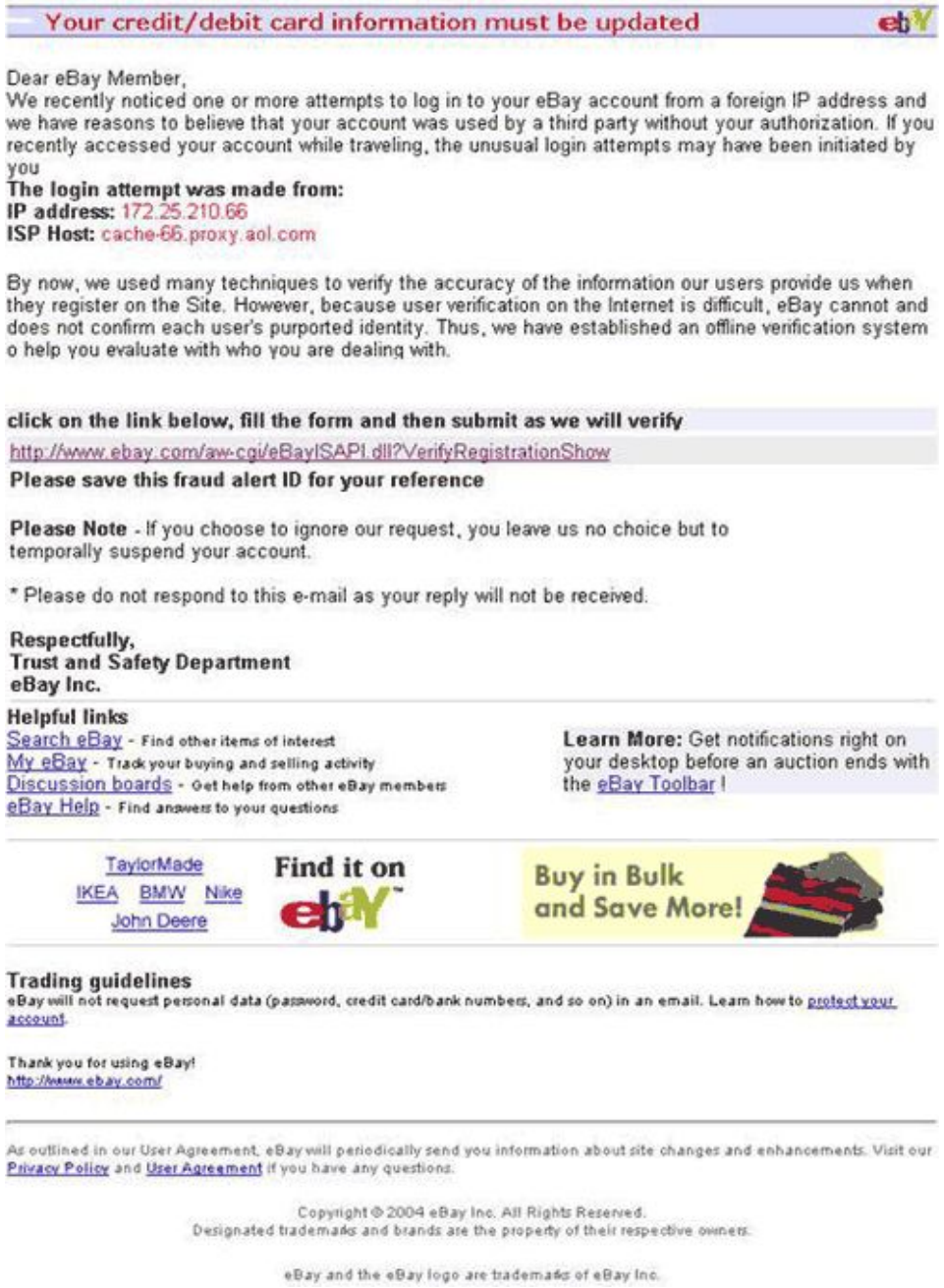
Вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Причины могут называться различные. Это может быть утеря данных, поломка в системе и прочее.

Фишинговые сайты, как правило, живут недолго (в среднем — 5 дней). Так как анти-фишинговые фильтры довольно быстро получают информацию о новых угрозах, фишерам приходится регистрировать все новые и новые сайты. Внешний же вид их остается неизменен — он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники.

Пример фишингового письма (подделка под уведомление интернет-аукциона Ebay)
со множеством ссылок, только одна из которых введет на сайт мошенников.

Наиболее частые жертвы фишинга — банки, электронные платежные системы, аукционы. То есть мошенников интересуют те персональные данные, которые дают доступ к деньгам. Но не только. Также популярна кража личных данных от электронной почты — эти данные могут пригодиться тем, кто рассылает вирусы или создает зомби-сети.



Your credit/debit card information must be updated

Dear eBay Member,
We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you
The login attempt was made from:
IP address: 172.25.210.66
ISP Host: cache-66.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system o help you evaluate with who you are dealing with.

click on the link below, fill the form and then submit as we will verify
http://www.ebay.com/aw-cgi/eBayISAPI.dll?VerifyRegistrationShow
Please save this fraud alert ID for your reference

Please Note - If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

* Please do not respond to this e-mail as your reply will not be received.

Respectfully,
Trust and Safety Department
eBay Inc.

Helpful links
Search eBay - Find other items of interest
My eBay - Track your buying and selling activity
Discussion boards - Get help from other eBay members
eBay Help - Find answers to your questions

Learn More: Get notifications right on your desktop before an auction ends with the eBay Toolbar !

TaylorMade
IKEA BMW Nike
John Deere
Find it on ebay
Buy in Bulk and Save More!

Trading guidelines
eBay will not request personal data (password, credit card/bank numbers, and so on) in an email. Learn how to protect your account.

Thank you for using eBay!
http://www.ebay.com/

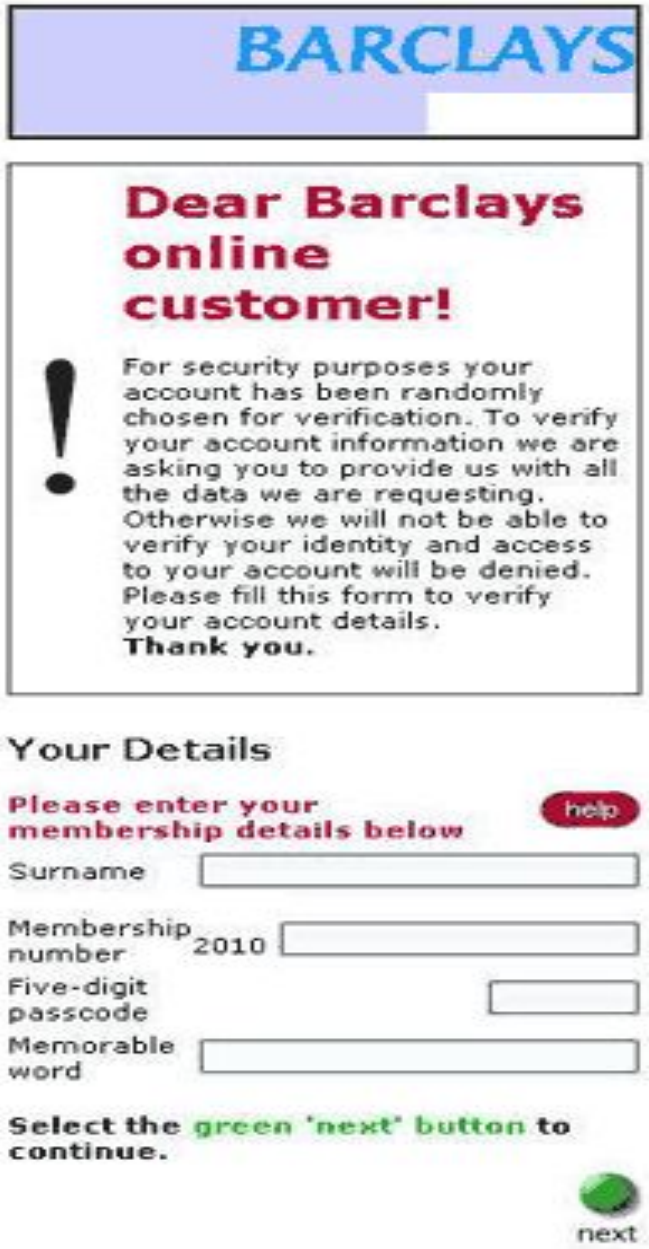
As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

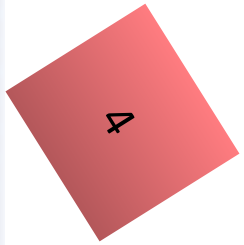
Copyright © 2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.

eBay and the eBay logo are trademarks of eBay Inc.

Пример фишингового письма (подделка под уведомление online-банка Barclays, где непосредственно в теле письма пользователь должен ввести свои данные).

Иногда личные данные предлагается ввести прямо в письме. Надо помнить, что никакой банк (либо другая организация, запрашивающая конфиденциальную информацию) не будет этого делать подобным образом.



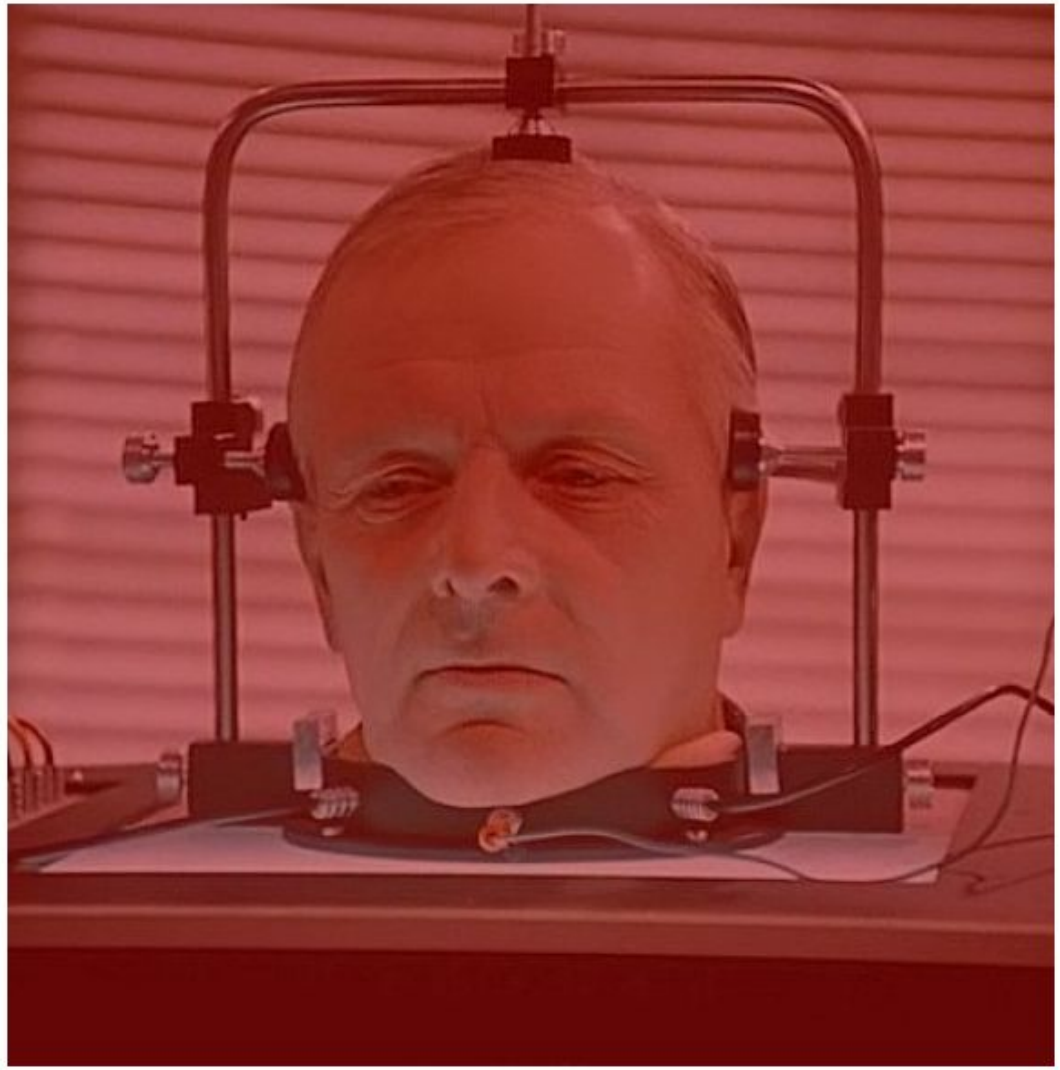


Кликбейт

(с англ. "click" — щелчок, "bait" — наживка) — это известные каждому сенсационные заголовки. Их цель — привлечь внимание читателя любыми способами, чтобы получить трафик. Именно из-за этого суть новости часто искажается, что приводит к ее недостоверности.

Пример кликбейта вы видите справа

В самом заголовке есть три признака кликбейта: местоимение “этот”, немотивированное использование многоточия и восклицательного знака, фраза “Ты не поверишь”. Ну и, конечно же, провокационная картинка, цель которой — привлечь внимание пользователя еще до того, как он прочитает заголовок.



Этот учёный защитил докторскую по нейробиологии... Ты не поверишь, чем он занимается теперь!

Сокращенные URL-адреса

Сокращатели URL – это сервисы, которые позволяют преобразовать длинные адреса в более короткие и удобные.

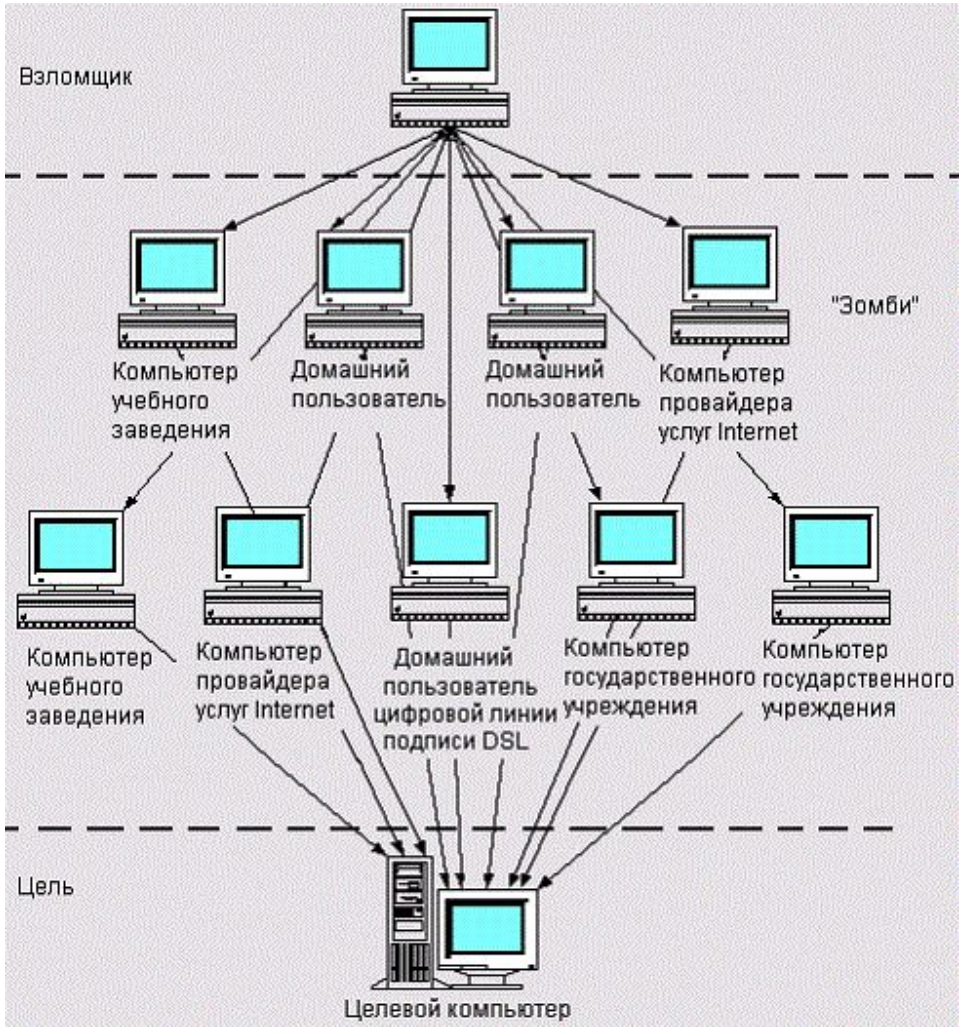
Зачем нужна короткая ссылка?

Компактная и визуально красивая ссылка является важной частью продвижения любого онлайн проекта. Сокращенная ссылка лучше запоминается, к тому же её удобно распространять среди пользователей. Пользуясь сжатым УРЛом можно следить за статистикой, включая анализ посетителей.

DoS и DDoS атака

хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.

В настоящее время DoS и DDoS-атаки наиболее популярны, так как позволяют довести до отказа практически любую плохо написанную систему, не оставляя юридически значимых улик.



Ботнет Mirai «Будущее» уже здесь

Mirai – это самораспространяющийся ботнет-вирус. Исходный код для Mirai был сделан общедоступным автором после успешной и широко разрекламированной атаки на веб-сайт Krebbs. С тех пор исходный код создавался и использовался многими другими для запуска атак на интернет-инфраструктуру

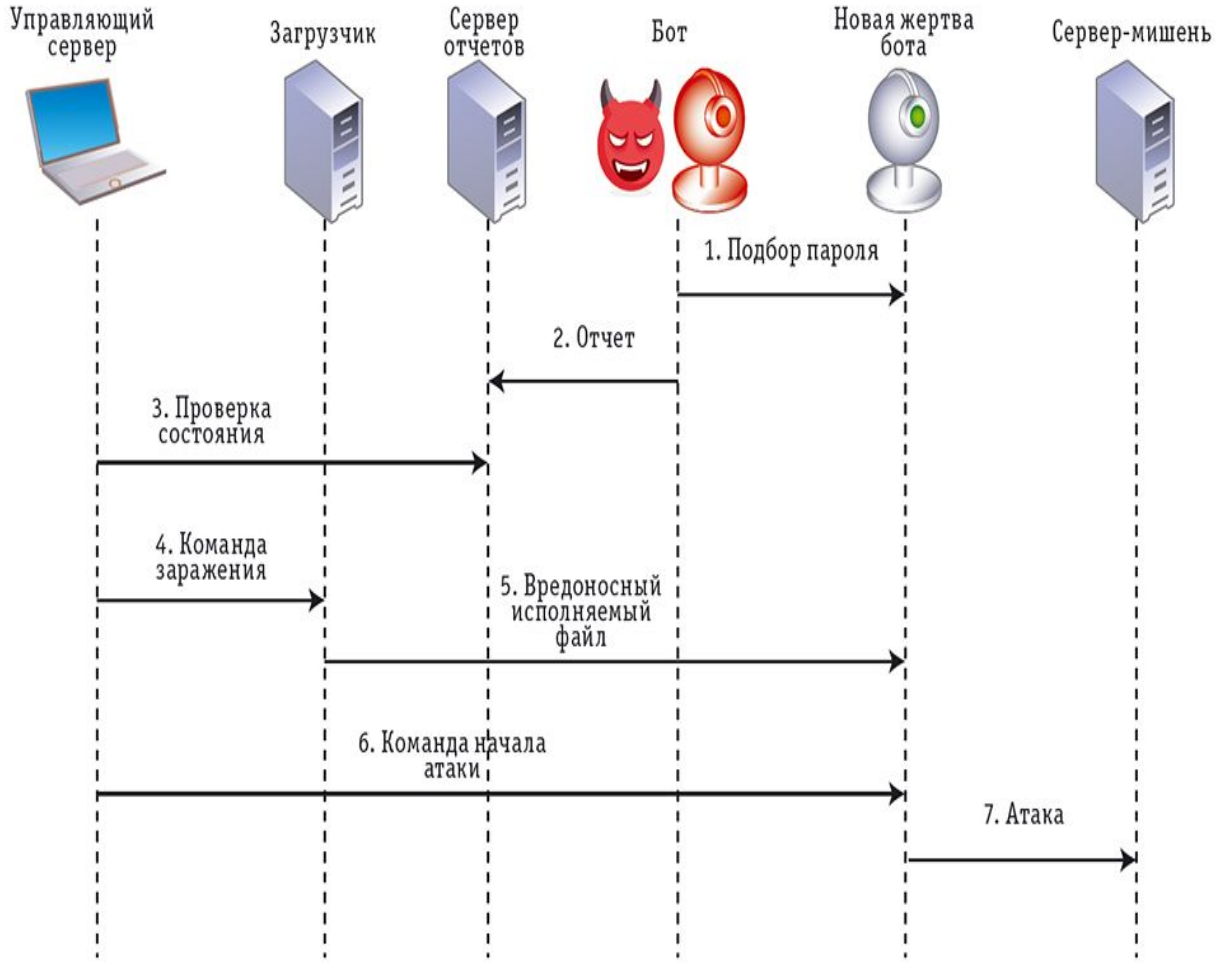
Mirai обычно распространяется, вначале заражая веб-камеры, цифровые видеорегистраторы, маршрутизаторы и т. д., на которых работает одна из версий BusyBox. Mirai устраивает DDoS-атаку против серверов-мишеней, активно распространяясь через устройства Интернета вещей с незащищенной конфигурацией.

Операции и потоки обмена данными в ботнете Mirai

1. Бот проводит атаку путем подбора, выясняя верительные данные устройств Интернета вещей, фабричные настройки которых не меняли. В словаре Mirai имеются 62 возможные пары «имя-пароль».

2. Обнаружив рабочие верительные данные и получив с их помощью доступ к командной строке или графическому пользовательскому интерфейсу устройства, бот передает его характеристики серверу отчетов через другой порт.

3. Боты начинают атаковать мишень, используя один из десятка доступных методов, среди которых флуд по протоколам Generic Routing



/ Напоминаю . НЕ ДОВЕРЯЙТЕ НЕЗНАКОМЦЕМ!!! \

Спасибо за просмотр!)