КИБЕРМОШЕННИЧЕСТВО (ИНТЕРНЕТ-МОШЕННИЧЕСТВО)

Интернет-мошенничество — это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получит доступ и каким-либо образом использует Вашу личную информацию, что предполагает мошенничество или обман. Виды интернет-мошенничества:

Фишинг

Фишинг (англ. phishing, от *fishing* — рыбная ловля, выуживание) — 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. Клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении («если вы не сообщите ваши данные в течение недели, ваш счет будет заблокирован»).

Фишинговые сайты, как правило, живут недолго (в среднем — 5 дней). Внешний же вид их остается неизменен — он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники.

Зайдя на поддельный сайт, пользователь вводит в соответствующие строки свой логин и пароль, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, в худшем — к электронному счету.

Еще одной хитростью фишеров являются ссылки, очень похожие на URL оригинальных сайтов. Они могут включать в себя название настоящего URL, дополненное другими словами (например, вместо www.examplebank.com стоит www.login-examplebank.com). Также в последнее время популярный фишинговый прием — ссылка с точками вместо слэшей, внешне очень похожая на настоящую.

Фарминг

Это тоже мошенничество, ставящее целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNS цифровые адреса легитимных веб-сайтов на адреса поддельных, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид мошенничества еще опаснее, так как заметить подделку практически невозможно.

Воровство конфиденциальных данных — не единственная опасность, поджидающая пользователя при нажатии на фишерскую ссылку. Зачастую, следуя по ней, можно получить программу-шпиона, кейлоггер или троян. Так что, если даже у вас нет счета, которым мошенники могли бы воспользоваться, нельзя чувствовать себя в полной безопасности.

Каким образом осуществляется интернет-мошенничество?

Многие интернет-аферы — это варианты мошеннических схем, существовавших еще до появления Сети, число которых увеличилось вместе с популярностью онлайн-шоппинга и других типов электронной коммерции. Для обмана пользователей интернет-мошенники используют электронную почту, чаты, форумы и фальшивые веб-сайты.

Как защитить себя от интернет-мошенничества?

Интернет-мошенничество и кража личных данных может произойти, если Вы отвечаете на спам-сообщения или на Ваш компьютер была запущена какая-либо вредоносная программа, позволившая хакеру получить к нему доступ. Лучшая защита от интернет-мошенничества — здравый смысл. Если предложение слишком хорошо, чтобы быть правдой, то это, скорее всего, обман!

- Не доверяйте любым нежелательным сообщениям, содержащим просьбу предоставить личную информацию.
- Игнорируйте спам.
- Никогда не предоставляйте Ваши персональные данные людям, в личности которых Вы недостаточно уверены.
- Запомните Ваши пароли и PIN-коды.
- Будьте очень осторожны при совершении онлайн-покупок, так как существует угроза фишинга, при которой мошенник может узнать номер Вашей кредитной карты. Используйте веб-сайты, которые обеспечивают безопасность сделок. Также, ознакомьтесь с политикой конфиденциальности сайта.
- Безопасность должна быть многоуровневой. Установите и регулярно обновляйте программные продукты, обеспечивающие безопасность Вашего компьютера (antivirus, antispyware и antimalware).

КУПЛЯ-ПРОДАЖА В ИНТЕРНЕТЕ

Каждый из нас хотя бы раз сталкивался с покупкой или продажей товаров в интернете. Но задумывались ли мы о том, что мошенники могут быть среди нас?

ДЕЙСТВИЯ МОШЕННИКОВ

Схема действий

Злоумышленники создают одностраничные сайты с подражанием обычным магазинам. Далее ничего сложного. Жертва оплачивает товар, а позже понимает, что остается у «разбитого корыта»

Отличительные признаки

- низкая цена
- нереальные условия сделки (доставка за 3 часа)
- отсутствие отзывов и контактной информации
- 100% предоплата

Наши действия

Нужно относиться внимательнее к выбору интернет-продавца и его магазину. Отслеживать отзывы о магазине или интересующем товаре.

ДОБРОВОЛЬНАЯ ПОМОЩЬ

Иногда мы встречаемся с тем, что кто-то нуждается в помощи окружающих. Это очень хорошо, что в нашей стране это действует на людей, и они готовы помогать нуждающимся. Но всегда ли всё на самом деле так, как мы видим?

ДЕЙСТВИЯ МОШЕННИКОВ

Схема действий

Мошенники составляют объявление о нужде в помощи и распространяют его на различных сайтах интернета.

Отличительные признаки

- Чаще всего у подобных псевдо-объявлений отсутствуют контактные данные

Наши действия

В первую очередь мы должны убедиться в подлинности объявления. Можно позвонить по указанному в объявлении номеру и познакомиться с родителями/контактным лицом. Это нужно для того, чтобы лично понять, действительно ли кто-то нуждается в помощи.

ВЫИГРЫШ В ЛОТЕРЕЮ

Каждый из нас, надеясь на свою удачу, хотел когда-нибудь выиграть без особых усилий какой-нибудь подарок судьбы. Кто-то этой наивностью однажды может воспользоваться.

ДЕЙСТВИЯ МОШЕННИКОВ

Схема действий

На ваш номер телефона приходит сообщение о том, что вы выиграли ценный приз в лотерее (смартфон, автомобиль). Далее вас просят перевести незначительную, в сравнении с призом, сумму на оформление доставки, документов и т. п.

Отличительные признаки

- отсутствие официального подтверждения
- неизвестная корпорация
- вымогательство денег

Наши действия

Нужно внимательно и с осторожностью относиться к таким сообщениям.

ФИШИНГ

Мошенники, совершая преступление, знают, что им от Вас нужно. Каждый вор знает, с какой стороны к Вам подойти.

ДЕЙСТВИЯ МОШЕННИКОВ

Схема действий

Мошенник представляется официальным представителем банка. Он просит Вас назвать ваши личные данные банковского счета, кодовое слово, пин-код, cvc-код, номер карты.

Отличительные признаки

- Мошенникам важна скорость. Они сообщают Вам о том, что ваши средства в опасности. И просят быстро принять решение.

Наши действия

Мы должны знать о том, что сотрудник банка не будет Вам звонить по такому поводу. Также стоит позвонить в банк и убедиться в целостности вашего счета.