

Материалы " PEOPLEnet против мошенничества"



Мобильный телефон и интернет

Без этих высокотехнологических вещей человек не может себя представить!



Современные технологии, давшие человечеству высокотехнологичные средства коммуникации, увеличили и возможности мошенников на поприще отъема денег.

Каждый пятый пользователь сотовой связи становится жертвой воришек!!!



Что делать? Как себя обезопасить?

Горячая линия «Мошенничество» – канал коммуникации с клиентами, созданный для получения и оперативного реагирования на сигналы о фактах мошенничества (как реализованного, так и потенциального)

Мошенничество – незаконные действия, направленные на завладение банковским имуществом, финансовыми ресурсами или собственностью путем обмана либо злоупотребления доверием.

Фрод (от англ. “fraud”) – другое название мошенничества, злоупотреблений, других деяний, связанных с несанкционированным доступом к материальным средствам.

MMS (Multimedia Message Service - служба мультимедийных сообщений) – система передачи сообщений с помощью мобильного телефона, содержащих мультимедийную информацию (звук, изображение, видео, анимацию и др.)

SMS (Short Message Service — служба коротких сообщений) – система приема и передачи коротких текстовых сообщений с помощью мобильного телефона.

Трафик (от англ. “движение, транспорт”) – объём информации, передаваемой по определенному каналу сети за определенный период времени.

Фишинг (от англ. “phishing”, от “fishing” — рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям



Материалы “PEOLEnet против мошенничества”

Фрикинг – несанкционированное получение информации (в т.ч. шпионаж) при помощи электронных устройств, а также путем несанкционированного подключения к телекоммуникационным сетям.

Компьютерный вирус – разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация). В дополнение к этому вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом.

Баннер (от англ. “banner” — флаг, транспарант) – графическое изображение рекламного характера, представляющее собой статическую или динамическую картинку и содержащее гиперссылку на ресурс рекламодателя.

Контент (от англ. “content” — содержимое) – любое информационно-значимое наполнение информационного ресурса.

Спам - массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений (информации) лицам, не выразившим желания их получать

“Короткий” номер – номер со специальной тарификацией, используемый для получения платных услуг, контента, как правило состоящий из 4-5 цифр



Смотри как интересно!!!!

открытки – поздравлялки, "а это не Ты на фотке?!!"

"посмотри/проголосуй, а то обижусь":

SMS интригующего содержания с просьбой отправить код на "короткий номер" и узнать тайну!



Познакомимся?! =)

Знакомство и флирт:

Всевозможные поводы знакомства с очаровательной девушкой/красивым парнем

SMS естественно платные!



Внимание! Изменились условия...

SMS от имени оператора связи с уведомлением об изменившихся условиях пользования услугами, для детальной информации предлагается отправить sms на "короткий" номер мошенников



Хочешь классную работу?!

Псевдоработодатели:

По контактам с публичных рекрутинговых сайтов ведется спам рассылка, о том, что Вы ну самая-самая подходящая кандидатура на престижнейшую работу! Детали по SMS на "короткий номер"



Хочешь бесплатно скачать файл?!

Пароль по SMS: Срочно необходима информация и она найдена! Нужно лишь отправить SMS на "короткий" номер и за символическую плату получить... еще одно SMS с уточняющими вопросами/просьбу подтвердить данные или другое.



Техночудо – ВАУ!!!

Самый полезные и незаменимые сервисы:

хотите получить эксклюзивную возможность: чтение чужих смс, слежение за абонентом, узнай историю рода, а у нас в базе Вы есть и др. – отправляйте SMS на "короткий" номер



Срочно пополни этот счет!

sms просьбы от имени родственников/близких друзей/коллег пополнить телефон, с которого пришло SMS

Повезло – Выигрыш!!!

Вы выиграли паразитальный приз! Одна деталь: перевести деньги на счет мошенников в банке / на «электронный кошелек», или активировать несколько карточек оплаты (при этом не самостоятельно активировать, а продиктовать номера карт организатору розыгрыша!

Ого, вот это акция!!!

заплати за чуть – чуть и получишь 100500 раз больше

Ой, ошибка! Переведи обратно, пожалуйста!

SMS – Вам пополнение счета! Далее SMS с неизвестного номера – с просьбой вернуть неправильно зачисленные средства. При чем, пополнение могло быть как настоящим(в дальнейшем платеж отменяется мошенником) так и фикцией.



Это ваш оператор! Вы ДОЛЖНЫ...

*Звонки от имени оператора моб. связи: у Вас заблокирован телефон или у Вас пропали средства со счета или тестирование новейшей услуги: купите карточку пополнения и активируйте по этому номеру;
перенастройка оборудования – наберите комбинацию(перевода средств на чужой номер)*



Здравствуйте, это Ваш банк! У Вас...

Звонки от имени банка: У Вас заблокирована карта или Вам отказано в кредите или у Вас похитили средства со счета. Далее распросы с выяснением конфиденциальной информации клиента.

Дозвонитесь, и оставайтесь на линии, пожааааалуйста!

мошенники всеми способами упрашивают потенциальных жертв позвонить на те или иные платные номера. Предлоги могут быть разнообразными: нужен донор для больного, нужно спасти бедных бездомных животных, телевикторины с сомнительными призами и др. В итоге такого звонка за незначительное время звонящий лишается внушительной суммы



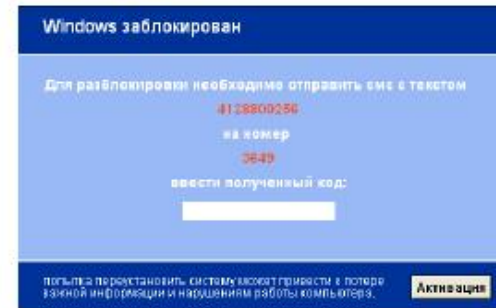
Баннеры "для взрослых"

Для просмотра контента эротического сайта нужна специальная программа, любезно предоставляемая авторами сайта(при чем даром!!). В дальнейшем, программа выводит на рабочий стол неудаляемую эросодержащую картинку/анимацию/видео для удаления которой нужен "выкуп"(обычно посредством SMS)



Блокираторы и шифровальщики

При переходе пользователей по непроверенным ссылкам и всплывающим окнам на компьютер/телефон устанавливается программа блокирующая OS. Разблокировка – посредством SMS.



Телефон самозвонилка/отправлялка sms

При заражении вирусом мобильный телефон, без участия владельца, совершает попытки звонков/SMS на платные номера, как правило международные



ЛЖЕантивирус

При просмотре сайта всплывает предупреждение об обнаружении вредоносных программ на компьютере и срочной необходимости проверки именно этим "антивирусом". По нажатию кнопки согласия на проверку на компьютер устанавливается вирус со вытекающими негативными сторонами



Хочешь работу? Реши задачу по ссылке...

Заражение вирусом связано с размещением резюме на рекрутинговых сайтах. Жертве приходит письмо по почте либо другому каналу связи о том, что он подходит работодателю и для понимания его профпригодности необходимо выполнить некое задание по ссылке. При переходе по указанному в сообщении линку происходит заражение компьютера/телефона вредоносной программой



РЕЗЮМЕ

"Волшебный кошелек"

По любым каналам связи (icq, e-mail, соц. сети) потупает спам с описанием якобы "дыры" в системе: при переводе на конкретный кошелек средств – владельцу возвращается удвоенная сумма.



ФИШИНГ

Вы получаете письмо по e-mail от имени Вашей платежной системы либо обслуживающего Вас банка с описанием какой – то насущей, важной для Вас проблемы (блокировка счета, подозрительные операции и т.д.). Для решения данных проблем дается указание зарегистрироваться по указанной ссылке. Письмо – фальшивка! После регистрации мошенники похитят Ваши средства с банковских!



Продажа по предоплате и бросовым ценам

Нашли в интернет объявления о продаже классных вещей и по классным ценам?!! От Вас то и требуется, что 50% предоплаты за товар!!! После перевода предоплаты: товара нет, покупатель так же пропал!



А есть телефон позвонить?!

Пользуясь доверием клиента злоумышленники, завладев телефоном могут разнообразным образом получить выгоду: банально убежать с телефоном в руках, позвонить или отправить SMS на один из платных "коротких" номеров и др.



Клонирование

С помощью специального оборудования есть возможность создать клон(аналог) карты. С помощью такого клона мошенник в дальнейшем будет систематически совершать звонки за ваш счет.



Мошенники ориентируются на схемы использования методов социальной инженерии на наименее опытных и защищенных пользователей.



Поэтому **проводите беседы с детьми, родственниками по повышению компьютерной грамотности и пониманию возможных угроз!**



Убедитесь в надежности ресурса, с которого производится загрузка файла;

Внимательно читайте условия предоставления сервиса(файла) – особое внимание обращайтесь на положения с ***

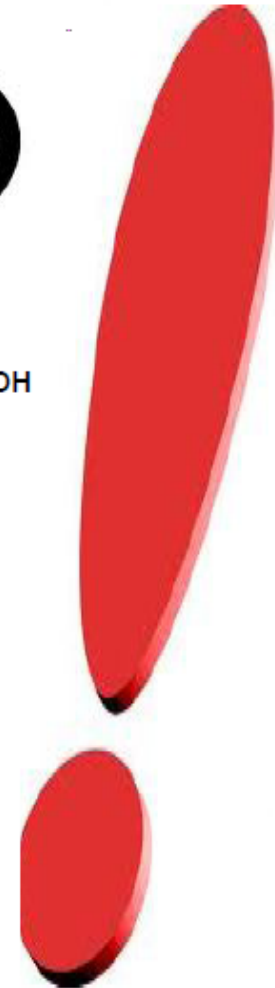
Не устанавливайте сомнительное ПО на свой компьютер/телефон

Не запускайте неизвестные вам установочные файлы

Проявляйте осторожность с всплывающими окнами/баннерами неизвестного происхождения(не переходите по таким ссылкам)

Не действуйте по указаниям программ блокираторов OS/шифровальщика файлов

Своевременно обновляйте антивирусное ПО(как на компьютере так и на телефоне)



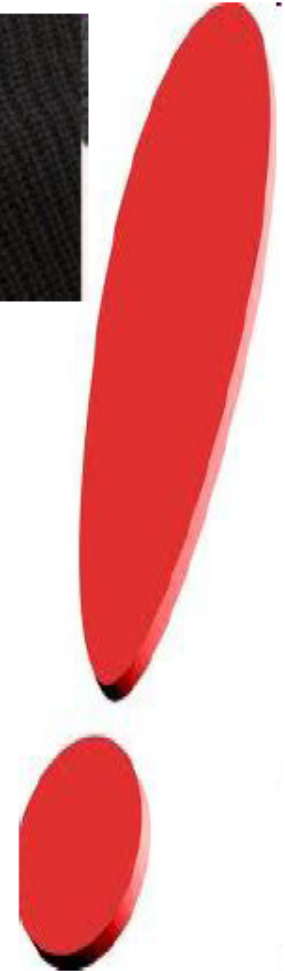
Следите за сохранностью конфиденциальной информации(номера банковских карт, PIN кода, пароли и т.п.)

Не переводите средства на номера, указанные в сообщениях от неизвестных Вам номеров

Просьба вернуть ошибочно переведенные средства – советуйте обратиться к оператору

Всегда связывайтесь с человеком, с которым якобы случилась неприятность

Не отдавайте телефон в руки незнакомых людей: нужно помочь – сами наберите номер и передайте необходимую информацию



уточняйте тарифы звонков на сервисные номера



при уведомлении о выигрыше – обращайтесь в к организаторам акций(радиостанции, телеканалы и т.д.)

При неотвеченных звонках не перезванивайте на незнакомые номера (особенно международные)

