[Советы по определению Интернет-ресурсов, несущих потенциальную угрозу финансовому благополучию пользователей]

Информация НЦБ Интерпола МВД России

о самых распространенных видах мошеннических действий с использованием компьютерных технологий.

Уважаемые граждане! Если Вы относитесь к активным пользователям Интернета, то рекомендуем Вам обязательно прочитать этот материал!

Мошенничество - это хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Подобная преступная деятельность преследуется законом независимо от места совершения - в реальной или виртуальной среде.

Мошенники постоянно изыскивают все новые и новые варианты хищения чужого имущества. Кратко остановимся на самых распространённых.

«Брачные мошенничества»

Типичный механизм: с использованием сети Интернет

преимущественно на сайтах знакомств преступники выбирают жертву, налаживают с ним электронную переписку от имени девушек, обещая приехать с целью создания в будущем семьи. Затем под различными предлогами «невесты» выманивают деньги (на лечение, покупку мобильного телефона, приобретение билетов, оплаты визы и т.д.). Переписка ведется главным образом студентами лингвистических ВУЗов. Направленные жертвами деньги преступники получают на подставных лиц. После получения средств переписка под различными предлогами прекращается.

«Приобретение товаров и услуг посредством сети Интернет»

Мы настолько привыкли покупать в интернет-магазинах, что часто становимся невнимательными, чем и пользуются мошенники. Обычно схема мошенничества выглядит так: создаётся сайт-одностраничник, на котором выкладываются товары одного визуального признака. Цена на товары обычно весьма привлекательная, ниже среднерыночной. Отсутствуют отзывы, минимален интерфейс, указаны скудные контактные данные. Чаще всего такие интернет-магазины работают по 100% предоплате. Переписка о приобретении товаров ведется с использованием электронных почтовых ящиков. По договоренности с продавцом деньги перечисляются, как правило, за границу через "Western Union" на имена различных людей. Конечно же, псевдо-продавец после получения денег исчезает!

«Крик о помощи»

Один из самых отвратительных способов хищения денежных средств. В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

Мы не призываем отказывать в помощи всем кто просит! Но! Прежде чем переводить свои деньги, проверьте - имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

«Фишинг»

Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

Так, с помощью спам-рассылок потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на "сайт-двойник" такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы. Достаточно распространенным является предложение о работе за границей, уведомление о выигрыше в лотереи, а также сообщения о получении наследства.

«Нигерийские письма»

Один из самых распространённых видов мошенничества. Типичная схема: жертва получает на свою почту письмо о том, что является счастливым обладателем многомиллионного наследства. Затем мошенники просят у получателя письма помощи в многомиллионных денежных операциях (получение наследства, перевод денег из одной страны в другую), обещая процент от сделки. Если получатель согласится участвовать, то у него постепенно выманиваются деньги якобы на оплату сборов, взяток чиновникам и т.п.

«Брокерские конторы»

С начала текущего года в НЦБ Интерпола МВД России наблюдается значительный рост количества обращений граждан, пострадавших от действий брокерских контор.

В распоряжении Бюро имеется информация о следующих недобросовестных брокерских компаниях: «MXTrade», «MMC1S» и «TeleTrade».

Для того, чтобы не потерять свои деньги при выборе брокерской компании необходимо обращать внимание на следующие признаки, которые характеризуют компанию-мошенника: обещание высоких процентов, отсутствие регистрации, обещание стабильной прибыли новичкам- трейдерам.

Перед тем, как доверить свой капитал, внимательно изучите не только интернет-ресурсы, но и официальную информацию о брокере и его регламент.

Важно! Помните, что инвестирование, предлагаемое на условиях брокерской компании, всегда является высоко рискованным даже при наличии безупречной репутации брокерской компании.

Безопасный Интернет детям

В МВД России дан старт всероссийской профилактической акции «Безопасный Интернет»

Урок, посвященный проблемам кибербезопасности, провели сотрудники МВД России в одной из столичных школ. К ребятам пришли в гости официальный представитель МВД России Ирина Волк, сотрудники УОС МВД России и Управления "К". Так был дан старт всероссийской профилактической акции для детей «Безопасный Интернет детям».

НОВОСТИ О ПРОВЕДЕНИИ УРОКОВ "БЕЗОПАСНЫЙ ИНТЕРНЕТ" В РЕГИОНАХ РОССИИ

«Представители МВД России в доступной форме рассказали школьникам об угрозах, поджидающих их на просторах Всемирной паутины, в частности, о новых видах кибермошенничества. Учащиеся узнали, каким требованиям должны соответствовать их пароли к личным аккаунтам в социальных сетях, на что следует обращать внимание при переписке с незнакомыми людьми, кто такие тролли и как правильно на них реагировать. Для некоторых стало сюрпризом, что за интернет-хулиганство может наступить реальная ответственность. В ближайшие недели аналогичные уроки будут проведены представителями территориальных органов МВД России в различных регионах страны», - сообщила Ирина Волк.

Сотрудники полиции объяснили ребятам, что обезопасить себя от большинства киберугроз не так уж и трудно. Достаточно серьезно отнестись к проблеме безопасности в виртуальной среде и следовать несложным правилам для защиты своих персональных данных, а своих компьютеров и гаджетов - от вредоносных программ. Особый акцент был сделан на необходимости соблюдения морально-этических норм в онлайн-общении и методах противодействия троллингу.

Завершением урока стал тест на киберграмотность, который практически все школьники прошли на «отлично».

Материалы для интерактивного урока, рассчитанного для школьников 11-14 лет, подготовили специалисты Управления «К» и УОС МВД России.

«Основные правила безопасности в сети Интернет»

Интернет – уникальная реальность нашего с вами времени. Это безграничный мир информации, где есть не только развлекательные и игровые порталы, но и много полезной информации для учебы. Здесь можно общаться со своими друзьями в режиме онлайн, можно найти новых друзей, вступать в сообщества по интересам. Информация, оперативно обеспечивающая ваши ежедневные потребности, - все это Интернет.

Почему же полицейские вынуждены предупреждать об опасностях виртуального мира, если в нем так много всего хорошего и полезного?

Достаточно большая часть интернет-пользователей ищет не друзей в Интернете, а свои жертвы.

Дело в том, что недобросовестные граждане - мошенники, наркодилеры, иные злоумышленники, асоциальные и психически нездоровые люди по-своему оценили возможности Интернета. Ведь именно Всемирная паутина дает возможность преступникам действовать анонимно.

Поэтому небезопасное поведение в сети Интернет может нанести вред и вам, и вашим родным и близким людям. Обезопасить себя не так уж и трудно – достаточно серьезно отнестись к проблеме кибербезопасности и соблюдать простые правила.

ТРИ самых общих правила, которые в наш информационный век должны стать вашими спутниками на всю жизнь:

1. ПАРОЛИ (ключ от дома)

Используйте всегда индивидуальные и сложные пароли, состоящие из букв, цифр и специальных символов. Исключите использование паролей по умолчанию, не сохраняйте пароли в ваших гаджетах и браузерах. Почему мы говорим об этом в первую очередь? Статистика говорит о том, что люди мало уделяют внимания парольной политике.

Третий год подряд самым популярным паролем в мире является «123456». Подобрать такой пароль к вашим порталам и персональным данным злоумышленнику не доставит труда.

Регулярно осуществляйте смену паролей, обеспечивая каждый раз их конфиденциальность. Это ваш самый большой секрет, как ключ от замка входной двери в ваш дом.

Правило первое: «Ключ от дома должен быть секретным, надежным, и только вашим, личным».

2. ВИРУСЫ и АНТИВИРУСЫ («моем руки с мылом»)

Любому компьютеру или гаджету могут навредить вредоносные программы (или вирусы). Они могут скопировать, повредить или уничтожить важную информацию, отследить ваши действия и даже украсть средства со счета. Программы «Черви», «Трояны», «Шпионы» - их множество разновидностей и красивых названий, а суть одна – все это вредные вирусы!

Для защиты компьютера на нем устанавливаются специальные защитные программы и фильтры. Использовать можно только лицензионное программное обеспечение с актуальными обновлениями.

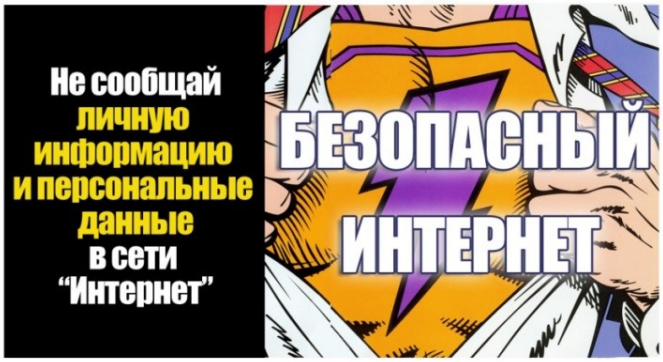
Устанавливать надо все обновления, как только они становятся доступными. Нельзя допускать истечения срока действия вашего антивируса.

Не качайте программные продукты из сомнительных источников (файлообменных сетей и торрентов). Не открывайте и не сохраняйте подозрительные файлы – сразу удаляйте. Не отвечайте на непонятные вам рассылки.

И главное - не посещайте ресурсы с сомнительной репутацией, которые вызывают у вас (или у вашей антивирусной программы) подозрения любого толка. Сомневаетесь – не нажимайте «да» или «ENTER».

Здесь можно провести простую параллель – держимся подальше от вирусов, моем руки регулярно, хорошим и качественным мылом. При любой сомнительной ситуации: «Моем руки с мылом, к вирусам не прикасаемся».

3. ПЕРСОНАЛИЗАЦИЯ (документы в сейфе)



Никому не передавайте свои конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес и прописку, и даже ваши фотографии. Такие «цифровые следы», если их создать, могут тянуться за вами всю жизнь. Могут навредить вам на пути к достижению поставленной цели. Игнорируйте в сети Интернет подобные запросы.

Получается странно – дома и на работе мы храним свои документы в сейфе, закрываем на ключ. Мы понимаем их важность. А потом по непроверенному запросу открываем сейф, достаем документы, фотографируем и посылаем посредством ресурсов в сети Интернет. Количество лиц, которые могут получить доступ к таким посланиям, даже трудно прогнозировать.

Давайте запомним третье правило: «Наши документы всегда в сейфе».