**Социальные сети**

Россия сегодня – лидер по времени, проводимому пользователями в социальных сетях.

Социальные сети «лишают» нас одиночества и скуки – там всегда есть с кем поговорить, обсудить только что вышедший фильм, похвастаться новым платьишком… Внутри соцсетей создаются профессиональные сообщества и группы по интересам, где можно узнать «за просто так» то, для чего в обычной жизни надо прочитать немало печатных текстов или прослушать курс лекций в каком-нибудь учебном центре, а иногда и найти настоящих реальных друзей. Форумы – площадки, создаваемые для обсуждения какого-то конкретного вопроса, и являющиеся более узким вариантом социальной сети, – позволяют быстро найти ответы на интересующие вопросы.

*Похищение сына известного российского предпринимателя было совершено весенним утром 2011 года в г. Москва рядом с офисом компании, где он работал программистом. Двое мужчин затолкали молодого человека в машину и увезли. Через некоторое время преступники потребовали у родителей похищенного €3 млн. за его освобождение. Родители похищенного обратились за помощью в полицию и через несколько дней молодой человек был освобожден в результате спецоперации, а его похитители были задержаны. Примечательно, что жертву для предстоящего похищения подбирали, руководствуясь списком самых богатых людей России, опубликованным журналом Forbes, а план разрабатывали исходя из информации, которую сын бизнесмена разместил в социальных сетях в интернете. Так, например, молодой человек опрометчиво указал в Сети место своего жительства, учебы и работы с адресами, писал о своем графике и маршруте следования от дома до работы.*

ОТСЮДА СЛЕДУЕТ ВАЖНОЕ ПРАВИЛО:

* Меньше конкретных данных о своей жизни.
* Не публикуйте информацию, по которой можно определить Ваш домашний адрес и время, когда там никого не бывает.
* Не размещайте в общем доступе посты о дорогостоящих покупках или сделках, в результате которых можно сделать вывод о наличии у Вас крупной суммы денег или ценностей, которые можно перепродать.
* Не описывайте свой постоянный маршрут, пролегающий между домом и работой – нападения с целью ограбления не всегда бывают случайными.
* Если очень хочется поделиться радостью от начинающегося отпуска, добавьте к сообщению приписку о включенной охранной сигнализации (даже если это неправда) – это наверняка отпугнет «продвинутых» любителей легкой наживы.

**Троллинг**

Троллинг – агрессивные, оскорбительные или провокационные комментарии в социальных сетях, призванные обидеть или разозлить автора «поста».

«Сделал гадость – сердцу радость» – тролль пишет, следуя именно этой поговорке. В критике тролля чаще всего нет ни грамма конструктива. Именно Ваше раздражение и огорчение доставляют ему наибольшую радость. Целью троллинга зачастую является привлечение внимания к себе – тролль хочет почувствовать свою значимость, произвести впечатление, даже если это впечатление резко негативное. Поэтому если на Ваш восторженный «пост» о Вашем родном районе Вы получить комментарий: «В этом районе живут только лохи!», знайте – к Вам в гости пришел тролль.

Не смотря на вроде бы небольшие масштабы проблемы, тролли могут создавать серьезный дискомфорт при общении в социальных сетях.

ЧТО ДЕЛАТЬ, КОГДА ТЕБЯ ТРОЛЛЯТ?

* Спорить с троллем, если ты сам не являешься еще большим троллем, бесполезно.
* Игнорируйте тролля, не отвечайте ему и не пытайтесь доказать, что он не прав. Не поддавайтесь искушению ответить троллю «железными аргументами». Задача тролля не найти истину, а вывести Вас из себя, поэтому большим разочарованием для него будет Ваше молчание в ответ.
* Можно «забанить» тролля – то есть внести его в Ваш личный «черный список». Для этого в некоторых соц. сетях есть специальные кнопочки, в других – необходимо обратиться к модератору.

**Электронная почта**

«СПАМ»

Спам – рассылка электронных писем (чаще рекламы) людям, не выражавшим желания их получать.

В общем-то, спам вполне безобидная штука, не приносящая особых неприятностей, кроме раздражения от замусоривания почтового ящика. Тем не менее, спам может быть опасен, важно, что у него внутри.

ПОЭТОМУ:

* Не поленитесь поставить галочку «защита от спама» в настройках вашего почтового ящика. Или хотя бы отмечайте такие письма как спам – это поможет вашей компьютерной почтовой программе распознавать спам еще на входе и не допускать его попадания в Ваш почтовый ящик.
* Никогда не отвечайте на спам и не переходите по указанным в нем ссылкам – это только даст понять спамерам, что на другом конце живой человек, и спровоцирует новый вал спама.

Электронная почта – отличный способ превратить Ваш компьютер в «бот» путем отправки Вам «трояна».

«БОТ» (сокращение от «робот») – компьютер, зараженный специальной программой, позволяющей злоумышленнику управлять таким компьютером по своему усмотрению без согласия владельца компьютера. Из бот-компьютеров создаются бот-сети (бот-неты), занимающиеся, например, рассылкой спама или атакой на ресурсы банков, и все это при полном неведении хозяев таких компьютеров.

«ТРОЯН» («троянская программа») – вредоносная программа (компьютерный вирус), проникающая на компьютер пользователя под видом безобидного приложения, с целью получить доступ к информации, размещенной на компьютере, или возможность удаленно управлять зараженной машиной.

ПРАВИЛА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ЭЛ. ПОЧТЫ:

* Не открывай подозрительные и «нежданные» письма с неизвестных электронных почтовых ящиков, и, что особенно важно, не открывайте вложенные в них файлы.
* Письма с неизвестных Вам электронных почтовых ящиков, с ящиков со странными названиями и заголовками в теме сообщения, такие, например, как «Мария Вездесущая. Ваше желание исполнилось», и присланные в них файлы надо безжалостно удалять, не поддаваясь соблазну посмотреть, что там внутри.
* Обязательно установите на компьютер антивирусную программу.

*Канадский водитель грузовика Джон Ремпел из Лимингтона попался на удочку «бездетного английского однофамильца, жаждущего осчастливить кого-нибудь из Ремпелов наследством в 12,8 миллионов долларов».*

*Для начала от Джона потребовалось 2,5 тысячи долларов, чтобы осуществить перевод, потом еще 5 тысяч на оформление дополнительных документов, потом еще 5 тысяч на открытие счета в лондонском банке, потом выяснилось, что нужно оплатить налог размером в 250 тысяч, который усилиями доброго адвоката скостили до 25 тысяч… Потом были еще расходы на авиабилеты, расходы за услуги транспортной компании и т.д,. и т.д. «Сломался» Джон на взятке в 12500 долларов сотрудникам Нью-Йоркского аэропорта – только после этого он решил обратиться в полицию.*

*Всего на эти манипуляции у канадца ушло около 150 тысяч долларов.*

Мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты от сумм. Если получатель письма, откликнулся и согласился участвовать, оказывается, что для получения «солидного куша» необходимо сделать самую малость – перевести немножко своих собственных денег на оформление сделки/уплату налогов/взятки чиновникам и т.п. Естественно в результате жертва так и не получает никаких миллионов. Сравнительно недавно появились и российские аналоги «нигерийских писем», в которых переписка ведется от лица несуществующего «российского бизнесмена», якобы нуждающегося в помощи адресата в переводе своего огромного состояния из России в другую страну (разумеется, за щедрое вознаграждение).

Кроме варианта с «богатым дядей» существует вариант с лотереей – жертве сообщается о крупном выигрыше в лотерею. Получатель письма должен заплатить (например, налог), чтобы получить свой выигрыш. (С похожей схемой работают «лохотронщики» на российских площадях и вокзалах, «впаривая» копеечные утюг/духи/косметику как приз, за который надо заплатить 1000 рублей налога).

Также существует онлайн-вариант брачной аферы, в котором мошенники ведут любовную переписку с целью «создания семьи». Суть мошенничества заключается в выманивании относительно небольших сумм «на билет и визу» для встречи с «любимым» или просто на «покупку веб-камеры».

Каков бы ни был вариант обмана при помощи таких «писем счастья»

СОВЕТ МОЖЕТ БЫТЬ ТОЛЬКО ОДИН: НИКАКИХ ДЕНЕГ!

Какими бы заманчивыми не казались предложения, помните: если у Вас попросили денег – Вас наверняка «разводят» (ну то есть пытаются обмануть на деньги). Не пересылайте, не занимайте и не давайте денег таким знакомым без основательной проверки полученной информации и нотариально заверенной расписки.

«ФИШИНГОВЫЕ ПИСЬМА»

Фишинговые письма – еще один способ мошенничества при помощи электронной почты – заключается в «выуживании» (по-английски fishing – рыбалка) у получателя письма информации, которую потом можно будет «монетизировать», например, адресов электронной почты других пользователей (их можно продать спамерам), паролей от других сервисов (социальных сетей, корпоративной электронной почты и т.д.).

На сегодняшний день преобладают фишинговые письма, направленные на получение от пользователя номеров и паролей его кредитных карточек или систем онлайновых платежей. Такие письма обычно маскируются под официальные сообщения от администрации банка, в которых сообщается, что получатель должен подтвердить сведения о себе (или срочно сменить пароль), иначе его счет будет заблокирован, и приводится адрес подставного сайта, внешне очень похожего на официальный сайт банка. Среди данных, которые необходимо ввести, есть и те, которые нужны мошенникам.

Чаще всего отличить «подставной» сайт от официального сайта банка «на глаз» практически нереально. Также простому пользователю очень сложно заметить разницу в доменных именах этих сайтов.

* Помните, банки или платежные системы НИКОГДА не запрашивают конфиденциальную информацию по электронной почте.
* Не переходите по ссылке, указанной в письме! Лучше наберите адрес сайта в браузере сами или найдите через поисковую систему (например, «Яндекс» точно знает официальные адреса сайтов крупных банков и умеет предупреждать о подозрительных сайтах).
* Внимательно читайте текст письма.
* Электронные письма от известных компаний не должны содержать орфографических или грамматических ошибок.
* Типичное фишинговое письмо начинается с обезличенного приветствия «Уважаемый пользователь» или обращения по адресу электронной почты. Ваш банк или платежная система обычно знает Ваше ФИО и в настоящем письме приветствует Вас, обращаясь по имени и фамилии (или имени и отчеству).
* Чаще всего мошеннические электронные письма содержат призывы к безотлагательным действиям (используя такие слова как «немедленно», «безотлагательно», «последнее предупреждение»), пытаясь заставить Вас действовать быстро и необдуманно.
* Не стесняйтесь позвонить в банк по номеру телефона, указанному на Вашей карте (именно на карте, а не указанному в письме или сайте, открывшемся по ссылке из письма, – там вполне может оказаться человек из команды мошенников) и все уточнить.
* Не пренебрегайте лицензионными антивирусами – многие из них блокируют фишинговые ссылки.
* Обращайте внимание на любые отклонения от обычного поведения Вашего банка (например, запрос новых сведений, которые раньше не надо было вводить). Если что-то идет не так как обычно, лучше отказаться от операции и перепроверить информацию у банка.
* Не пренебрегайте возможностью услуги «смс-оповещение» от банка – если деньги начнут внезапно утекать с Вашего счета, будет шанс успеть заблокировать карту.

ВЗЛОМ ПОЧТЫ.

Здесь важно знать, что, если кто-то очень хочет взломать Вашу почту (впрочем, как и входную дверь Вашей квартиры) он это сделает. Это только вопрос времени и затрат ресурса человеческого или компьютерного (современные хакеры давно автоматизировали процесс взлома – это и быстрее, и следов меньше).

КАК ОНИ ЭТО ДЕЛАЮТ?

1. Подбор пароля.

Это самый простой (и самый используемый) способ вскрытия электронного почтового ящика. Для этого даже не надо быть программистом – в сети гуляет множество программ, которые подставляют в качестве пароля определенные слова (или сочетания символов) используя при этом готовые словари.

2. Подсматривание пароля.

Подбор пароля – удел хакеров. А вот подсмотреть пароль, записанный на листочке, может случайно зашедший в гости сосед/коллега. Хорошо, если его любопытство ограничится просмотром Ваших фоток… Ну дальнейшее развитие событий можете додумать сами.

СОБЛЮДАЙТЕ ПРАВИЛА РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ:

* Не храните в электронном почтовом ящике (особенно на бесплатном почтовом сервисе) ценную информацию, секретные документы и интимные фотографии. После пересылки или скачивания обязательно удаляйте такие письма. При необходимости переслать ценную для Вас информацию, воспользуйтесь программой шифрования, а код от шифра сообщите собеседнику другим способом, например, по телефону.
* Не используйте для паролей простые общеупотребимые слова.
* Никто не любит сложных паролей, так как их легко забыть, но если Вы не хотите, чтобы Вашу почту взломали хакеры, то правило - «чем сложнее пароль, тем выше безопасность» - именно для Вас.
* Если у Вас несколько почтовых ящиков, не используйте на всех один и тот же пароль. Пусть он будет отличаться на 1-2 символа, но это может спасти Вас от утечки всей информации.
* Не ленитесь периодически менять пароли, особенно в случае появления подозрения о том, что текущий вариант пароля скомпрометирован.
* НИ В КОЕМ СЛУЧАЕ не записывайте пароли в блокнотике, который лежит «под рукой» возле монитора компьютера.

**Интернет(онлайн)- банкинг или мобильный банк**

*В апреле 2015 г. Управлением «К» МВД России при содействии экспертной организации и службы безопасности Сбербанка задержаны российские участники одной из киберпреступных групп. Злоумышленники организовывали вирусные атаки на мобильные устройства клиентов российских банков. Троянская программа, которую они использовали, после установки на мобильное устройство запрашивала баланс привязанной к номеру банковской карты, скрывала поступающие SMS-уведомления и осуществляла переводы денежных средств с банковского счета на счета, подконтрольные злоумышленникам.*

*На основании полученных данных удалось установить личности четырех жителей Челябинской области, подозреваемых в совершении преступления. У задержанных было изъято несколько ноутбуков, полтора десятка сотовых телефонов и большое количество SIM-карт.*

Для безопасности денежных средств:

* если у вас к счету мобильного телефона привязана банковская карта, то в случае утраты мобильного телефона обязательно и срочно блокируйте не только сим-карту, но и банковскую карту (в крайнем случае позже ее можно будет разблокировать).
* поставьте на Ваш смартфон антивирусное приложение.

ДОПОЛНИТЕЛЬНО

Процесс придумывания (и главное, запоминания) сложных паролей можно упростить, если вспомнить, что наши клавиатуры имеют две раскладки – русскую и латинскую. Например, простой пароль «password» можно переиначить в «gfhjkm», то есть русское слово «пароль» набрать в латинской раскладке клавиатуры. А можно еще больше усложнить задачу по подбору пароля путем использования целых фраз, заменяя пробелы между словами какими-либо специальными символами (например, пароль «мама мыла раму» легко трасформируется в «vfvf$vskf$hfve$»). Добавляем смену регистров (большие и маленькие буквы), цифры и сильно осложняем дело хакерам.