Главное управление по вопросам безопасности
Губернатора и Правительства Хабаровского края

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВОПРОСАМ ПРОФИЛАКТИКИ ИНТЕРНЕТ-МОШЕННИЧЕСТВ (ДЛЯ ИСПОЛЬЗОВАНИЯ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ)

г. Хабаровск, 2018 год

ВВЕДЕНИЕ

Сегодня Интернет - это всемирная сеть, количество пользователей которой превышает 4 млрд. человек и их количество продолжает неоспоримо расти.

В наше время каждый второй ребенок умеет пользоваться благами современной цивилизации. По последним исследованиям самым популярным среди россиян является мобильный Интернет - около 91,4 млн. человек. При этом в зависимости от возраста ребенка определяются его потребности в Интернет ресурсах.

Поэтому, для обеспечения безопасности детей во "Всемирной паутине" необходимо использовать современные способы воздействия на детей посредством Интернета, иными словами, комплексно подходить к формированию культуры безопасности жизнедеятельности подрастающего поколения, как дома, так и в образовательных организациях.

Просвещение подрастающего поколения в части использования различных информационных ресурсов, знание элементарных правил отбора и использования информации способствует развитию системы защиты прав детей в информационной среде, сохранению здоровья и нормальному развитию.

Медиаобразование выполняет важную функцию защиты от противоправного и манипулятивного воздействия средств массовой коммуникации, а также способствует предупреждению криминальных посягательств на детей с использованием информационно-телекоммуникационных сетей.

Что делает среднестатистический пользователь в Интернете? Ищет информацию, скачивает музыку и фильмы, пишет в блог, посещает развлекательные сайты, пользуется почтой и т.п.

Но вот однажды он сталкивается с заманчивым предложением заработать энную сумму денег за короткое время. Неважно, что именно ему предлагают, в его голове уже начинают крутиться мысли о легком заработке. Даже если он достаточно осторожен и не доверяет всему, что пишут, качественный дизайн и грамотный текст могут развеять все его сомнения.

Что уж говорить о неопытных подростках… Человек отсылает нужную сумму на кошелек или проводит какие-то другие действия, и терпеливо ждет. Мошенник же получает свои деньги.

Мошенничество в Интернете приобретает все большие масштабы. Изобретаются все новые уловки по выкачиванию денег с простодушных пользователей. Анонимность мошенников, большое количество доверчивых людей – все это подпитывает такой вот своеобразный вид "бизнеса".

За 8 месяцев 2018 года на территории Хабаровского края зарегистрировано 380 фактов мошенничеств, совершенных с использованием средств мобильной связи (за тот же период 2017 года – 264, рост составил 43,9%), из которых раскрыто 23,4% (8 месяцев 2017 г. – 13,9%).

Количество фактов мошенничеств, совершенных с использованием пластиковых карт, электронных платежей, сети интернет составило 355 (8 месяцев 2017 г. – 427), из которых раскрыто всего 10,1% (8 месяцев 2017 г. – 24,8%).

За тот же период на территории нашего края зарегистрировано 160 краж денежных средств, совершенных с использованием средств мобильной связи (8 месяцев 2017 г. – 94, рост – 70,2%), из которых раскрыто 48,7% (8 месяцев 2017 г. – 39,8%).

Количество краж, совершенных с использованием пластиковых карт, электронных платежей, сети интернет составило 96 (8 месяцев 2017 г. – 97), из которых раскрыто всего 25,3% (8 месяцев 2017 г. – 30,6%).

Нельзя не отметить и высокий уровень латентности данного вида преступлений, ведь далеко не каждый пострадавший от рук мошенников обратится с заявлением в полицию, особенно если у него похитили всего пятьсот или тысячу рублей.

"Погружаясь" в виртуальный мир, большинство пользователей просто забывают о том, что в Интернете действуют те же законы, что и в жизни. Сейчас редко найдешь человека, который бы попытался выиграть у наперсточника на вокзальной площади, а вот когда ему же предложат отослать деньги на так называемый "волшебный" кошелек, с тем, чтобы потом получить удвоенную сумму, все защитные психологические барьеры вдруг оказываются снятыми, и он с радостью соглашается.

Главное, что нужно помнить всем – "халявы" не бывает. Никто никогда не даст денег просто так. Деньги не появляются из неоткуда, даже если они "электронные". А Интернет – это просто средство передачи информации.

ВИДЫ МОШЕННИЧЕСТВ В ИНТЕРНЕТ-СЕТИ

В теории каждый знает, что бесплатный сыр бывает только в мышеловке и далеко не всем людям стоит верить на слово, однако в реальной жизни многие об этом полностью забывают и с легкостью идут на поводу у аферистов. Именно на это, а также на незнание основных схем обмана уповают интернет-мошенники подыскивая новых жертв.

В общем и целом большинство схем обмана в сфере онлайн-платежей можно разделить на следующие группы.

Мошенничества, связанные с Интернет-покупками.

Самая примитивная, но от того не менее "эффективная" методика изъятия денег у доверчивых граждан - получить средства, не предоставив товаров и услуг взамен.

Через Интернет вам могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно.

Нередко люди теряют деньги, покупая вещи на липовых интернет-аукционах или в интернет-магазинах. Вы просто перечисляете деньги

за покупку, а товар не приходит. Вы заранее оплачиваете услуги специалиста, а он не приезжает. И тому подобное.

К сожалению, ни опыт, ни разум, ни осторожность не могут защитить вас на 100% в случае бесконтактной сделки.

Однако, соблюдая некоторые правила покупки товаров через Интернет, можно оградить себя от возможных неприятностей.

- Вас должна насторожить слишком низкая цена на определенный товар, а также отсутствие фактического адреса или телефона продавца. Скорее всего, вам предлагают приобрести подделку либо хотят присвоить ваши деньги.
- Не поленитесь позвонить продавцу по телефону и подробнее выяснить уже известные вам особенности товара, его технические характеристики и т.д. Заминки на другом конце провода или неверная информация, которую вам сообщили, должны стать поводом для отказа от покупки в данном Интернет-магазине.
- Наведите справки о продавце, изучите отзывы о его работе, и только после этого решайте - иметь ли дело с выбранным вами Интернет-магазином.
- Пользуйтесь услугами курьерской доставки и оплачивайте стоимость товара по факту доставки.

Еще один эффективный способ: проводить проверку с помощью сетевого сообщества. Свойство интернета стремительно проводить информацию здесь играет против аферистов. В ответ на запрос по ключевым словам поисковик выбросит десятки отзывов с рунетовских форумов, которые станут исчерпывающей характеристикой для домена, аукциона или предложения о работе.

Фишинг (от англ. fishing - рыбная ловля, выуживание) - вид интернет-мошенничества, цель которого - получить данные, содержащиеся на вашей пластиковой карте.

Аркадий продавал лодку за 250 000 рублей. Вывесил на одном из общеизвестных ресурсов объявление. Через неделю позвонила пожилая женщина, сказала, что купит лодку и готова внести предоплату.

Все, что для этого нужно, - номер карты продавца. Наш продавец продиктовал номер. Посыпались СМС-сообщения из банка. Он не беспокоился, потому что в этот момент его жена отдыхала за границей и могла делать покупки с того же счета.

Через некоторое время пожилая дама позвонила и попросила назвать код, который должен прийти из банка, уверив нашего героя, что беспокоиться не о чем: *"Это же я вам оплачиваю. Что может случиться?"*

В результате со счета Аркадия сняли 1 100 000 рублей.

Мошенники пытались снять деньги с карты. Банк, как и полагается, высылал владельцу карты код безопасности для проведения операции. Но, несмотря на все предупреждения, несмотря на то, что в самом СМС-

сообщении с кодом банки просят никому не сообщать этот код, Аркадий все равно это сделал.

Рекомендация тут одна: **максимально внимательно относитесь к требованиям безопасности, предлагаемым вам банками.**

На самом деле все подобные вышеописанной операции методики специалисты называют общим термином — **фишинг**, то есть выуживание у жертвы секретных данных о его счетах, что и позволяет опустошить эти счета за считаные секунды.

Помимо мошеннических покупок и продаж в настоящий момент фишинговая схема чаще всего работает так:

1. Вы получаете СМС-сообщение или электронное письмо с информацией о том, что ваш банковский счет заблокирован по неким уважительным, но независящим от вас причинам.
2. Вас просят перезвонить по указанному номеру или перейти по ссылке.
3. В обоих случаях вас просят сообщить номер карты, имя, код безопасности и код безопасности операции, высылаемый банком при совершении операции.
4. В ближайшие минуты ваш счет опустошают настолько, насколько это возможно при установленных банком или же вами самим ограничениях.

Другой тип фишинга имеет целью получить не деньги, а ваш интернет-ресурс, аккаунт.

1. Вам приходит письмо о попытке взлома ресурса или каких-то технических проблемах и просят сообщить код.
2. После этого ваш ресурс перехватывают и используют в собственных целях.

К сожалению, методов фишинга невероятно много. И мошенники придумывают все новые, более изощренные. Так что 100%-ной защиты тут тоже не существует. Есть лишь рекомендации, позволяющие снизить риски.

Главное правило во всех подобных случаях — не горячиться.

Необходимо продумать, как проверить информацию. Скажем, спокойно позвонить в банк, связаться с провайдером, если речь идет об интернет-ресурсе. Они тут же прояснят ситуацию.

Причем связываться нужно не по тем каналам, которые предоставлены в сообщении, а по тем номерам и адресам, которые указаны у вас в договоре, на карточке банка и т. п.

Следует помнить, что банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить свои данные. Если такая ситуация произойдет, вас попросят приехать в банк лично.

Интернет-попрошайничество.

Этот вид надувательства встречается прежде всего в социальных сетях, но может попадаться и баннерная реклама.

Многим пользователям периодически попадаются слезные мольбы родителей или доброхотов пожертвовать денег на лечение смертельно больного ребенка, несчастной красавицы, замечательного человека, спасти животных из распущенного приюта, которым грозит усыпление, и тому подобное.

В конце поста обычно приводятся номера счетов, на которые можно положить деньги (часто это просто "Яндекс-кошелек", WebMoney и другие способы быстрого перевода денег без реквизитов), и просьба перепостить информацию.

Причем ссылки, указанные в постах, часто приводят к сайтам, где описываются вполне реальные случаи, взятые из баз данных благотворительных фондов и гуманитарных организаций.

Получается, что несчастные люди и животные вполне реальны. Только счета указаны совсем не те.

Тут надо понимать, что, если деньги собирает официальная организация, информацию о конкретном случае можно и нужно проверить.

- благотворительные сборы не осуществляются при помощи личных или безымянных счетов.

- банковский счет всегда имеет банковские реквизиты, содержащие отнюдь не номер карточки, а номер счета получателя, корреспондентский счет, БИН, ИНН и КПП банка.

- ну и, конечно, организация должна подтвердить, что этот счет верный.

Для того чтобы не попасться на крючок и не отдать свои деньги в руки мошенников не поленитесь перезвонить в указанную организацию, уточнить номер расчетного счета либо посетить ее лично, убедиться в достоверности размещенной информации, выяснить все подробности дела, а затем уже решать - передавать деньги или нет.

Что касается сбора денег частными лицами, тут обычно может помочь лишь общение. Серьезные жертвователи не посылают денег, если нет телефона получателей. Часто даже короткий разговор позволяет понять реальные намерения.

Помимо желания обогатиться те, кто размещают подобные объявления, часто это делают для увеличения своей аудитории при помощи перепоста ложной информации.

Полученную аудиторию они перепродают каким-либо компаниям для маркетинговых целей или используют их для раскрутки своего аккаунта или сайта.

Подбери интернет-кошелек

"Хочу поделиться секретом! Нашел в Сети волшебный кошелек. Попробовал отправлять на него 100 рублей - через четыре часа вернулось

200! Это чума - какой-то глюк в системе Яндекс.Деньги. Только быстрее надо, пока админы не запалили".

Любому здравомыслящему человеку ясно, что такое предложение - обман на пустом месте. Почему совершенно незнакомый человек, вместо того чтобы тихо собирать "золотые" с веток, вдруг делится секретом со всей Паутиной? Но находятся простаки, и в волшебные кошельки летят все новые виртуальные сторублевки.

В секретных посланиях факт существования таких кошельков объясняется по-разному. Глюк системы, рекламная акция, заначка для непредвиденных расходов крупной фирмы. Бывают совершенно издевательские варианты. Например, кошелек якобы принадлежит мошенникам. "Верный способ. Давайте разорим их всем миром". Или еще: Яндекс хочет поддержать репутацию и вернуть потери обманутым. Платеж просто надо пометить: "Я был обманут кошельком N XX". Администратор якобы проверит и вернет сумму потери.

Следующая ступень - виртуальные обменники. "Доброжелатель" опять же ни с того ни с сего делится секретом. Якобы на разнице курсов электронных валют можно неплохо заработать . Меняя от 20 единиц за один раз (меньше обменник якобы не берет), можно зарабатывать два доллара с каждой операции. Сначала меняешь, к примеру, web-money на E-gold, потом обратно - в секретном интернет-обменнике, который дает выгодный курс, потому что хочет "раскрутиться" и стать известным. В день можно заработать 400-500 долларов.

Не исключено, что один-два раза такая финансовая операция может действительно пройти. До тех пор, пока вы тестируете систему 20 долларами. И хотя владелец "зеленых" понимает, что в реальности с обменниками такая схема не пройдет, трудно побороть искушение. И тогда секретный обменник перестает подавать признаки жизни.

Деньги на спасение бизнеса

Некий интернет-магазин предлагает вам вложить некоторую, обычно не слишком большую сумму для пополнения оборотного капитала. Мол, на данный момент кредитов не хватило, а товары закуплены, площадка готова к обслуживанию покупателей, но не хватает лишь малости — скажем, 1 500 000 рублей. Обещают вернуть через месяц на 300–500% больше.

В результате оказывается, что это финансовая пирамида, в которую заманивают людей под видом вложений в реальный бизнес. Риск потерять деньги в этом случае так же велик, как и в любой пирамиде.

Звони бесплатно

Бесплатная мобильная связь - неизбежность. Развитие телекоммуникаций приведет нас именно к такому положению вещей. Каналы связи будут бесплатными. Люди будут платить за доступ к контенту.

Однако будущее еще не наступило. Тем не менее, мошенники предлагают вам бесплатную связь уже сегодня. За 3000–5000 рублей вам

предлагают установить на телефон "особую прошивку", позволяющую совершать звонки бесплатно.

Обычно это объясняется несовершенством биллинговых систем операторов. Естественно, личный контакт с провайдером подобных услуг невозможен. Деньги переводятся на интернет-кошельки. Однако и после "установки" прошивок пользователи продолжают исправно платить по счетам компаний связи.

Коварные СМС

Если вам необходимо скачать в сети некий контент - программу, музыку, фильм, книгу и тому подобное, - любой поисковик выведет вас на сайты, где вам предлагается скачать требуемый контент бесплатно.

1. Вы нажимаете кнопку "скачать", и тут обнаруживается, что вам нужно ввести свой телефонный номер и нажать кнопку "продолжить".

2. После этого вам сообщают, что на указанный номер послано СМС-сообщение, на которое вы должны ответить, подтверждая факт вашего существования, после чего контент скачается.

3. Вы отвечаете.

4. С вашего телефонного счета уходит значительная сумма денег.

Точно такие же случаи бывают со скачанными уже архивами, которые не распаковываются без этой процедуры, фильмами, музыкой.

Главная и единственная рекомендация в данном случае - не отвечайте на СМС-сообщение. Требование предоставить номер для отсылки вам какого-то кода - вещь обычная. Но это одностороннее общение. Вы получаете код и вводите его в поле оболочки ресурса. Так что никогда не отвечайте на СМС!

"Победитель" лотереи

Вам сообщают, что вы выиграли в лотерею, но нужно перевести небольшую сумму на оформление, пересылку, административные расходы.

Помните: в лотерею нельзя выиграть, если вы в ней не участвовали!

ЗАКЛЮЧЕНИЕ

К сожалению, мошенники — люди опытные, тратящие немало времени на продумывание своих действий. Обычные же люди, какими бы разумными они ни были, никогда специально не готовятся к столкновению с обманом. Поэтому мошенники всегда находятся на более сильных позициях.

Из-за свойственного им опыта и мастерства распознать их намерения непросто.

Так что если у вас просят денег - **не давайте.**

Если вас вовлекают в незнакомую схему - **не участвуйте.**

Если вас пытаются купить на жалость или жадность - **не ведитесь хотя бы сразу**. Чаще всего взывание к страстям и эмоциям - это манипуляция. Или хотя бы не давайте деньги сразу, подумайте, не торопитесь. Или давайте, но тогда ни о чем не жалейте.

Кстати, иногда деньги в Сети люди просят совсем не мошенническим путем, но руководствуясь принципом "А вдруг?"

"Прошу пожалуйста перечислите на карты *(....)* СКОЛЬКО СМОЖЕТЕ, хоть 10000 р., А самое наилучшее, нужно около 7–8 млн.! Вообщем сколько сможете! Это не шутка! Говорю честно! Очень нужно для семьи по Ипотеке и серьезным кредитам! И очень хотим хорошую недорогую машину! Заранее спасибо огромное! Очень нужно! Серьезно. Неприятная история произошла с этой ипотекой. Перечислите пожалуйста! Просто реально помогите обычным людям! Я на двух работах работаю и ничего не получается. Извините что вот так прошу, самой стыдно как не знаю кому. Перечислить можно в любом отделении втб или сбербанка. Если чем могу помочь — звоните! Мария и Алексей".

Не исключено, что кто-то дал денег этим "страдальцам".