Единый урок по безопасности в сети Интернет (сентябрь-ноябрь 2018)

Интернет - мошенничество

Мошенничество (или в простонародье – лохотрон) – это обманный способ добычи денежных средств или других ценностей, основанный на доверчивости граждан.

Фишинг

- Фишинг или выуживание персональной информации, работает по следующей схеме. На Вашу электронную почту приходит сообщение о том, что Вам срочно необходимо обновить или передать Ваши персональные данные, в какой-либо системе.
- Например, Вам приходит письмо о том, что произошел какой-то сбой, и данные по Вашей банковской карте повреждены или утеряны и просят прислать их им заново. Сообщение Вам приходит, как правило, с угрозой блокировки счета или аккаунта.

Блокировщики windows, баннеры мошенников

- Если Вы работаете в интернете на компьютере без антивируса или с устаревшими базами, Вы можете заразить свой компьютер вирусом. Одним из видов мошеннических вирусов является блокировщик Windows.
- Вирус попадает на Ваш компьютер, как правило не заметно и автоматически, а дальше он добавляет свой код в автозапуск системы.
- В итоге сразу или после перезагрузки компьютера Windows блокируется баннером с сообщением о необходимости отправки смс на номер … . При этом как правило содержатся угрозы о уничтожении данных.
- Отправка смс в таком случае пустая трата денег. Компьютер от этого не разблокируется. Для разблокировки системы можно поискать код в интернете или на сайтах производителей антивирусных программ. Если же ничего не получается то остаётся только переустановить систему Windows заново. Поэтому лучше держите важную для себя информацию на диске D или стороннем носителе.

Попрошайничество

- В основном таким видом мошенничества в интернете занимаются люди просящие не большие суммы денег под различными предлогами. Это может быть и помощь бездомным животным, а может и срочная операция ребёнку.
- Суммы, как правило, просят не большие (так больше шансов их получить), а за счёт охвата большого количества народу они собирают вполне приличные деньги. Для такого вида мошенничества используется спам или социальные сети.
- Конечно, может быть и реальный случай, когда людям действительно нужна помощь. В таком случае постарайтесь максимально проверить эту информацию, узнать ФИО, связаться по телефону, узнать, обращались ли они в известные благотворительные организации и т.д. В общем, будьте бдительны!

Лёгкие деньги, мгновенный заработок.

- Заработать огромные деньги, потратив минимум времени и вложений обещает «Форекс», онлайн казино, букмекерские конторы и т.д. Интернет просто кишит лозунгами «Мы научим Вас зарабатывать миллионы» и т.п. Как пример встречаются такие баннеры:

Взломы аккаунтов

- **Мошенники могут взломать вашу страничку в социальной сети** и потребовать послать смс на платный короткий номер при Вашей попытке входа в аккаунт.

- Ни в коем случае не стоит этого делать. За смс с Вас снимут не менее 300 рублей, а для разблокировки вашего аккаунта достаточно указать Ваш номер мобильного и Вам на него придет смс с Вашим новым паролем. Эта операция совершенно бесплатна. Если Вы в чем нибудь, сомневаетесь сразу, обращайтесь в службу поддержки.

Интернет мошенники и электронные кошельки

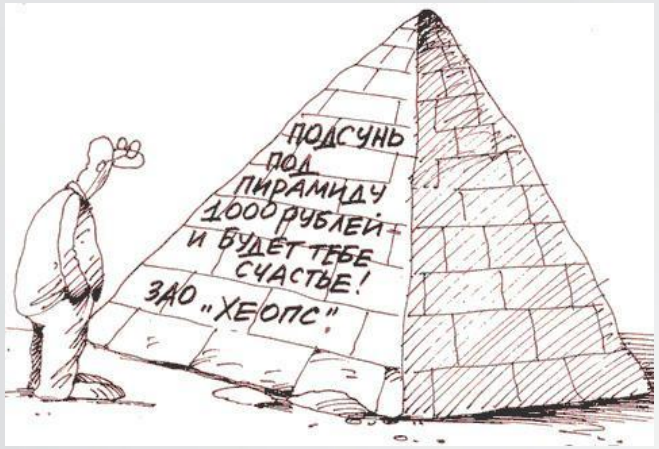
- На сегодняшний день все больше людей заводят себе электронные кошельки. Это удобные и безопасные средства расчётов в сети интернет. Самые популярные из них: WebMoney, Яндекс.Деньги, Qiwi кошелёк и т.д.
- **Мошенники** активно используют e-mail рассылку от имени тех. поддержки той или иной платёжной системы. Обычно в письме говорится, что Ваш интернет кошелёк заблокирован (или может быть заблокирован, или требуется его повторная активация и т.п.) и Вам необходимо пройти по ссылке ниже, где ввести свои личные данные (логин, пароль). Причём и e-mail адрес отправителя данного письма может соответствовать адресу Вашей тех. поддержки, и страница на которую Вы попадаете, перейдя по ссылке из письма, будет такой как на официальном сайте.
- Нужно чётко понимать, что официальная тех. поддержка никогда не будет спрашивать у Вас идентификационные данные (логин, пароль).
- Если Вам пришло такое письмо, рекомендуется зайти на официальный сайт компании Вашей платёжной системы и написать письмо в службу безопасности, подробно описав проблему.

Программы для взлома различных платежных систем

- В интернете полно объявлений о суперпрограммах, которые якобы могут взломать любой электронный кошелек. Купив такую программу за деньги, Вы в лучшем случае получите не рабочий софт. В худшем вирус на Ваш компьютер.

СМС (SMS) лохотрон в интернете.

- Вам приходит sms сообщение, что якобы кому-то из Ваших близких (сыну, дочери и т.д.) срочно нужна помощь и что бы её оказать Вам необходимо положить деньги на определённый номер. Казалось бы, **чистой воды лохотрон**, но подобные сообщения обычно приходят поздно вечером, ночью или рано утром и от неожиданности многие люди, не дозвонившись до своих близких попадаются на него.



Финансовые пирамиды

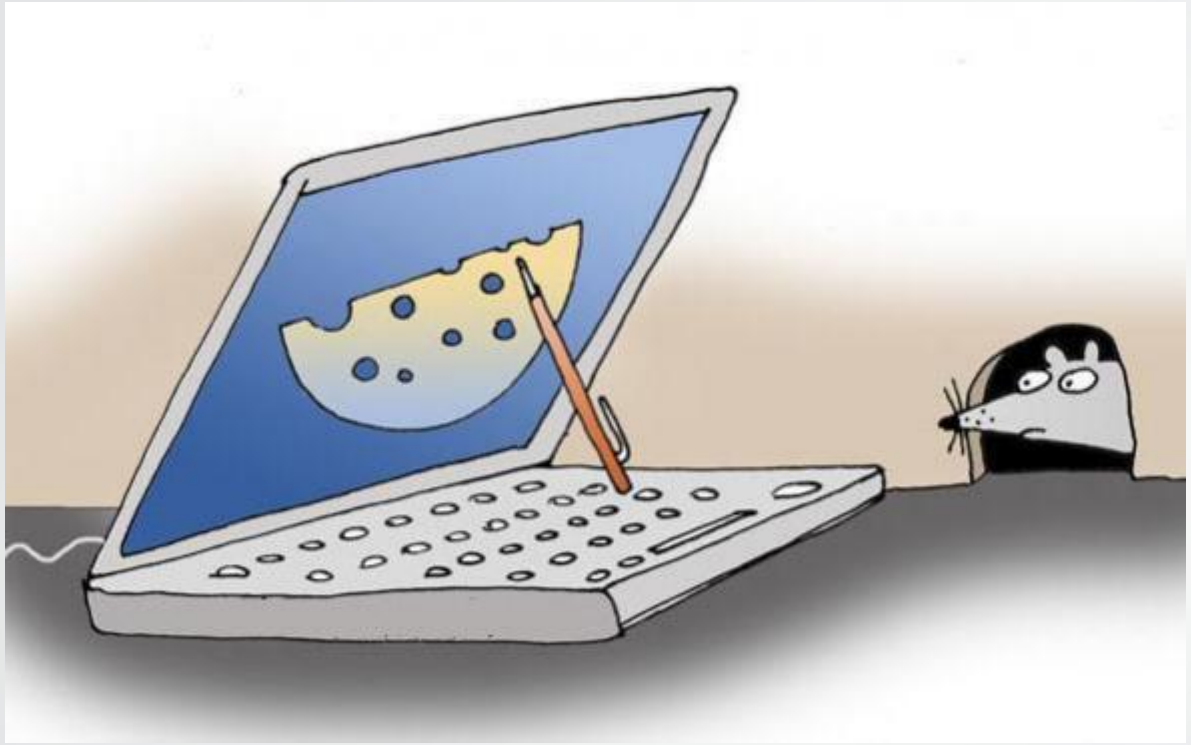
- В сети встречается большое количество объявлений различных финансовых пирамид, где за небольшую плату Вам обещают сказочный заработок, который напрямую зависит от количества привлечённых Вами партнеров.
- К подобного рода финансовым пирамидам относятся разные маркетинговые компании (MLM) торгующие товарами, в которых нет собственно никакой необходимости. В 95% случаев люди, вступившие в финансовую пирамиду, просто теряют своё время и деньги!

КАК НЕ СТАТЬ ЖЕРТВОЙ ИНТЕРНЕТ МОШЕННИКОВ?

- Основными **признаками мошенничества** являются:
- навязчивая реклама, обещающая огромный доход без вложения знаний и большого труда;
- требование ввода ваших персональных данных на сомнительных ресурсах;
- требование отправки смс;
- заманчивые предложения, приходящие через почту от незнакомых людей. Как правило, это спам.

Чтобы не потерять свои деньги и время:

- Работайте в интернете с хорошей антивирусной программой;
- По возможности задавайте сложный пароль на сайтах где хранится важная для Вас информации или Ваши деньги;
- Не отправляйте смс на незнакомые номера или делайте это предельно осторожно, проверив сначала истинную стоимость смс;
- Не вступайте в сомнительные компании, в которых сначала нужно платить, а потом якобы огромная прибыль (Форекс, MLM);
- Не пытайтесь зарабатывать используя разные лохотроны такие как букмекерские конторы, электронные казино и т.д.;
- Прежде чем сделать какую-нибудь покупку на неизвестном для Вас сайте, поищите отзывы о нем и его товаре, почитайте форумы. Проверьте сайт на наличие персонального аттестата продавца WebMoney, проверьте, работают ли контактные телефоны.



Будьте бдительны!
Не станьте жертвой интернет – мошенников!