БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ ДЛЯ ЗАЕМЩИКОВ!

Одним из наиболее распространенных видов хищения путем обмана является мошенничество в сети Интернет, поскольку в современном обществе без Интернета уже не обойтись.

Данная разновидность мошенничества является наиболее опасной и серьезной, поскольку в сети зарегистрировано огромное количество людей, и преступления могут совершаться на дальних расстояниях. О том, как не пострадать от мошенничества в Интернете и куда обращаться, поможет данная статья.

Обращаем ваше внимание, что последнее время значительно участились случаи мошенничества в интернете с использованием логотипов известных компаний. Недобросовестные сайты вводят пользователей в заблуждение, выманивая деньги и персональные данные.

КОМПАНИЯ FINPOINT ОБРАЩАЕТ ВАШЕ ВНИМАНИЕ!

- Мы никогда не требуем отправки сообщений. Мы сами отправляем смс с кодом подтверждения.
- Мы никогда не отправляем сообщения с просьбой подтвердить, обновить или предоставить персональные данные.
- Оформление займов онлайн и доступ в личный кабинет возможны только по ссылкам на официальном сайте https://finpoint.ru/
- Обязательно проверяйте адрес сайта, прежде чем вводить логин и пароль.
- На сайте https://finpoint.ru/ указаны контактные данные и реквизиты организации.

ОСНОВНЫЕ ТИПЫ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

Интернет-фишинг

Это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Зачастую это рассылка электронных писем либо личных сообщений, например, от имени банков или внутри социальных сетей. В письме часто содержится ссылка на сайт, внешне неотличимый от настоящего. Пользователь вводит свой логин и пароль, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

SMS мошенники

Отправка смс на бесплатный номер. Как показывает практика – номер оказывается более чем платным и одно сообщение может обойтись в 100, а то и более рублей.

Электронные кошельки

Один из видов мошенничества заключается в том, что Вам на e-mail приходит письмо о том, что Ваш кошелек заблокирован и необходимо перейти по какой-либо ссылке и ввести персональные данные. Ни в коем случае делать этого не стоит! Все проблемы, связанные с электронными кошельками, решайте только при помощи службы поддержки.

Взломы аккаунтов

Мошенничество здесь заключается в том, что при попытке входа в социальную сеть для разблокировки своего аккаунта Вас просят отправить смс на какой-либо номер. Ни в коем случае не делайте этого! Для разблокировки аккаунта необходимо ввести номер телефона, на который придет смс с кодом подтверждения.

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ

1. Не отправляйте смс на короткие номера или делайте это очень осторожно, проверив истинную стоимость смс
2. Работайте в сети с качественной антивирусной программой
3. Регулярно обновляйте операционную систему и установленные в ней приложения, воспользуйтесь функцией автоматического обновления
4. Не открывайте файлы и не переходите по ссылкам, пришедшим Вам в сообщениях электронной почты, мессенджерах, социальных сетях и других программах для обмена сообщениями (Skype, WhatsApp, Viber и т.п.) от незнакомых или подозрительных лиц и компаний
5. Проверяйте антивирусной программой файлы, полученные из сети Интернет или со съемных носителей (флеш-карт) до их использования
6. Установите запрет на установку мобильных приложений из ненадежных источников
7. Установите на свое устройство пароль из сложноподбираемых символов, не используйте в качестве пароля свою дату рождения, номер телефона и другие данные, доступные неопределенному кругу лиц
8. Не вступайте в компании, в которых нужно сначала платить
9. Используйте на своем устройстве автоматическую блокировку экрана на позднее чем после 10 минут бездействия устройства
10. Не используйте сайты в сети Интернет, при взаимодействии с которыми не осуществляется шифрование передаваемых данных, следите чтобы адрес web-страницы начинался с символов https. Символы http без последней буквы S говорят о том, что данный сайт не использует безопасную передачу данных. Не игнорируйте предупреждения о нарушении безопасности вашим браузером
11. Не пытайтесь зарабатывать на различных финансовых пирамидах, таких как казино, букмекерские конторы и других сомнительных ресурсах
12. Прежде чем что-либо приобрести на неизвестном Вам сайте, проверяйте полную информацию о нем, поищите отзывы, почитайте форумы
13. Не сообщайте свои персональные данные неизвестным лицам и сомнительным организациям
14. Храните свои пароли в недоступном для третьих лиц месте и не сообщайте их никому
15. Если вы получили подозрительное смс-сообщение либо зашли на сайт, имитирующий сайт компании finpoint.ru, просим вас незамедлительно связаться с нами по номеру горячей линии, либо писать на электронную почту info@finpoint.ru

КАК ЗАЩИТИТЬ СВОЙ АККАУНТ В ПОРТАЛЕ "ГОСУСЛУГИ"

1. Используйте уникальный пароль

"Госуслуги" требуют от вас придумать длинный и сложный пароль, чтобы его было труднее подобрать. Однако сервис никак не может проверить его уникальность. Если вы воспользуетесь тем же самым паролем, которым защитили электронную почту и еще десяток аккаунтов на других сервисах, то утечка данных с любого из них поставит ваши документы под угрозу.

Поэтому для такого важного аккаунта, как на «Госуслугах», не только рекомендуется, но и жизненно необходимо придумать уникальный пароль.

2. Включите оповещения о входе в ваш аккаунт Госуслуг

Если вы включите оповещения, то после каждого успешного входа вам придет письмо на электронную почту. Так вы узнаете, если кто-либо, кроме вас, получит доступ к аккаунту, и сможете своевременно поменять пароль. Чтобы включить уведомления о входе:

- Нажмите на свою аватарку и в открывшемся меню выберите Настройки и безопасность.

- В блоке Вход в систему включите оповещение на электронную почту о входе в систему.

3. Задайте контрольный вопрос

Контрольный вопрос — это дополнительная мера защиты от попыток посторонних сменить пароль от вашего аккаунта. Но стоит помнить, что контрольный вопрос не защитит вас, если ответ на него легко угадать или найти в Интернете. Важно, чтобы его знали только вы, причем могли в любой момент его вспомнить.

Чтобы задать контрольный вопрос:

- Нажмите на свою аватарку и в открывшемся меню выберите Настройки и безопасность.

- В блоке Вход в систему выберите Контрольный вопрос, введите Ваш вопрос и ответ на него, подтвердите активацию функции паролем для входа на портал Госуслуг, нажмите Включить.

4. Включите двухэтапную проверку входа

После включения двухэтапной проверки, чтобы войти в вашу учетную запись, злоумышленнику потребуется ввести не только пароль, но и одноразовый SMS-код, который придет на ваш телефон. Таким образом, вы будете в относительной безопасности, даже если ваш пароль украдут. Заодно вы вовремя узнаете о том, что пароль попал не в те руки, и сможете оперативно сменить его.

Чтобы включить двухэтапную проверку:

- Нажмите на свою аватарку и в открывшемся меню выберите Настройки и безопасность.

- В блоке Вход в систему выберите Вход с подтверждением по SMS, нажмите Настроить. - Удостоверьтесь, что на экране отображается Ваш номер телефона, и подтвердите активацию функции паролем для входа на портал Госуслуг.

5. Включите вход с помощью электронной подписи

Если вы пользуетесь квалифицированной электронной подписью, можно применять ее и для входа в аккаунт. Этот метод надежнее SMS-кодов: перехватить сообщение с одноразовым кодом проще, чем подделать подпись.

Нажмите на свою аватарку и в открывшемся меню выберите Настройки и безопасность.

В блоке Вход в систему выберите Вход с помощью электронной подписи.

Подтвердите активацию функции паролем для входа на портал Госуслуг и нажмите Включить.

Если электронной подписи у вас нет, безопаснее отказаться от этой опции: без ЭЦП она бесполезна, а включая ее, вы теряете возможность получать коды через SMS.