ПРОТИВОДЕЙСТВИЕ ИТ-МОШЕННИКАМ

IT-преступления, или киберпреступления – это противоправные действия, совершаемые с использованием информационных технологий. Они могут быть направлены против отдельных лиц, организаций или государств.

ОСНОВНЫЕ ВИДЫ МОШЕННИЧЕСТВА:

1. Взлом аккаунта

Если вы получаете сообщение с просьбой об одолжении денег или сборе средств для благотворительности, то убедитесь, что это реальный человек, спросите у него что-то, что знает только он, либо просто игнорируйте такие сообщения.

2. Кликбейт

Кликбейт – захватывающий заголовок, который прерывается на самом интересном месте, и вас отсылают читать продолжение в источнике. В большинстве случаев кликбейт относительно безопасен – скорее всего вас просто перенаправит на страницу с рекламными баннерами. Однако такие новости могут быть опасными, потому что туда можно вложить ссылку с опасным контентом.

3. Выигрыши

Баннер, картинка или плашка от браузера, где заявляется, что ваш IP-адрес был выбран в качестве победителя.

4. Платные опросы

Если вы видите такие предложения, то обратите внимание на предлагаемую сумму, если вам предлагают заработать 25 тысяч рублей за опрос — это обман.

5. Спам

Такие письма почти гарантированно содержат в себе вирус. Вы получаете спам-письмо, переходите по ссылке и дальше идет цепная реакция — одна ссылка перенаправляет на другую (а таких перенаправлений может быть сколько угодно много) и рано или поздно вы получите вирус или требование ввести личные данные.

6. Документы и файлы

В документах могут содержаться макросы. Они потенциально очень опасны. Поэтому если вы не пользуетесь макросами, то вам лучше отключить их исполнение в настройках офисных программ.

7. Фишинг

Фишинг — один из видов интернет-мошенничества, основанный на принципах социальной инженерии, целью которого является обманом вынудить пользователя совершить необходимые злоумышленнику действия. Многие фишинг-атаки незамысловаты и легко выявляются. А некоторые могут быть весьма изощренными, поэтому следует проявлять здоровую дозу скепсиса, чтобы отсеивать подозрительные письма, ссылки и сообщения. Чтобы не попасться на типовые фишинг-атаки, руководствуйтесь приведенными ниже рекомендациями.

Важно помнить, что IT-преступность – это серьезная проблема, которая требует внимания и принятия мер для защиты себя и своих данных

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ:

- Установите на телефон (компьютер) лицензированное антивирусное программное обеспечение.
- Не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных сайтов, присланные по электронной почте (подозрительные файлы лучше сразу удалять).
- Используйте пароли, не связанные с Вашими персональными данными.
- Не сообщайте данные карты, пароли и другую персональную информацию.
- Поставьте лимит на сумму списаний или перевода в личном кабинете банка.
- По всем возникающим вопросам обращайтесь в банк, выдавший карту.
- Не выполняйте никаких срочных запросов к действию, в том числе по установке каких бы то ни было приложений.
- Не перезванивайте по номерам и не переходите ни по каким ссылкам, которые приходят на e-mail или по SMS.

Общие правила для сотрудников

- защитите ваши соцсети;
- не переходите по подозрительным ссылкам;
- не вводите данные от страницы на сторонних ресурсах;
- не давайте ваш смартфон посторонним.

Общие правила для защиты соцсетей

- Если в соцсети вам пишут с аккаунта банка или другой организации, проверьте аккаунт на официальном сайте или по телефону банка/компании. Если такого аккаунта там нет, не отвечайте на сообщения и заблокируйте подозрительный аккаунт.
- Не доверяйте в соцсетях тем, кто просит у вас деньги, даже если просьба пришла от вашего друга. Позвоните тому, с чьей страницы пришло сообщение, и уточните, действительно ли ему нужны деньги. Если нет – не отвечайте мошеннику, заблокируйте его и пожалуйтесь в службу безопасности соцсети.
- Проверяйте все файлы, которые приходят в личных сообщениям. Если прикреплен файл с расширением .exe (надпись в конце названия файла), это странно – не открывайте файл.
- Периодически проверяйте, когда последний раз ваш аккаунт был активен. Если появились подозрения, завершите все активные сеансы и смените пароль.

Как реагировать на странное электронное письмо

- Не переходите по ссылкам в письмах от незнакомцев, не нажимайте на картинки и кнопки;
- если отправитесь представляется сотрудником компании, но пишет не с корпоративной почты, а с обычной, например, mail.ru или gmail.com, не открывайте письмо;
- не верьте в обещания внезапных выигрышей и не попадайтесь на попытки вас запугать;
- не открывайте вложенные файлы из писем незнакомцев, как бы заманчиво они ни выглядели. Не скачивайте файлы типа *.exe, *.scr, *.bat, *.vbs;

- видели странный адрес в письме, например, с ошибкой в доменном имени, – удалите письмо.

Как реагировать на подозрительный звонок

- Мошенник может представиться сотрудником банка, покупателем, который хочет приобрести вашу вещь по объявлению, представителем компании, сообщающим о крупном выигрыше и т.п.;
- не сообщайте никому данные вашей банковской карты, особенно CVC-код, особенно по телефону незнакомцу;
- если вам уже пришло СМС с кодом, не сообщайте его никому, особенно «сотруднику банка» – настоящие банковские служащие не будут спрашивать у вас такие данные;
- закончите разговор. Если человек представился сотрудником банка, позвоните в ваш банк, обрисуйте ситуацию и сообщите телефонный номер мошенника для проверки.

Вы попали на подозрительный сайт

- Не переходите по ссылкам, не нажимайте на подозрительные и кричащие картинки;
- не верьте обещаниям внезапных выигрышей и не попадайтесь на попытки вас запугать;
- если сайт неопрятный, кричащий, с грубыми ошибками в текстах и большим количеством уведомлений, всплывающих окон и призывов перейти или оставить данные, скорее всего, сайт фишинговый. Закройте вкладку и не возвращайтесь на него;
- прежде чем ввести свои данные на сайте, убедитесь, что это нужный сайт: клоны иногда выглядят очень похожими на оригинал. Проверьте адрес несколько раз. Если что-то в нём вас смущает – закройте вкладку;
- регистрируйтесь и покупайте только на сайтах с SSL-сертификатами безопасности и двухфакторной аутентификацией. Чтобы зайти в личный кабинет, вас проверят по двум параметрам: помимо логина и пароля у вас спросят, например, код из СМС;
- если перед адресом сайта вы видите HTTP, а не HTTPS и ваш браузер сообщает о ненадёжности страницы – он прав. Сайты без SSL-сертификатов лучше обходить стороной.

Рекомендации для повседневной жизни

- Не указывайте личную информацию в открытых источниках. Адреса, даты рождения, номера телефонов: ваши и членов вашей семьи. Всё это может помочь мошенникам узнать пароль или секретное слово, взломать ваши аккаунты и получить доступ к деньгам и данным;
- меняйте пароли не реже, чем раз в полгода. «Я вообще не меняю пароли, и меня ни разу не взломали. Зачем начинать?» – спросите вы, и это будет ошибка выжившего. Соблюдая правила, вы усложните работу преступникам, ведь никто не знает, когда на его деньги и данные может начаться охота;
- не используйте одинаковые пароли для всех ваших аккаунтов. Не давайте мошенникам ключ от всех дверей. Мошенник, узнавший пароль от одного вашего аккаунта, сразу же попробует открыть этим ключом остальные ваши кабинеты, и

он подойдёт. Не рискуйте всем и проявите фантазию, придумывая новые комбинации;

- используйте режим инкогнито в браузере, когда работаете за чужим компьютером, заходите в свои аккаунты и вводите личную информацию. Когда вы закроете вкладку браузера, ваши пароли и данные не сохранятся, а выход из всех аккаунтов произойдёт автоматически;
- включите двухфакторную аутентификацию во всех ваших аккаунтах, потому что такой тип защиты надёжнее убережёт вас от атак мошенников – чтобы взломать ваш аккаунт, им придётся преодолеть двойной барьер. И это будет непросто;
- установите антивирус на все ваши устройства.