Что такое киберпреступность?

Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов.

Киберпреступления совершают частные лица и организации – от начинающих хакеров до слаженных группировок, которые используют продвинутые методики и хорошо подкованы технически.

Какие есть типы киберпреступлений?

Вот некоторые разновидности киберпреступлений:

- Мошенничество с использованием электронной почты и интернета
- Кража цифровой личности (хищение и использование личных данных)
- Кража данных платежных карт и другой финансовой информации
- Хищение и перепродажа корпоративных данных
- Кибершантаж (вымогательство денег под угрозой атаки)
- Атаки с использованием программ-вымогателей (одна из разновидностей кибершантажа)
- Криптоджекинг (майнинг криптовалют с использованием чужих ресурсов)
- Кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным)
- Нарушение работы систем с целью компрометации сети
- Нарушение авторских прав
- Незаконное проведение азартных игр
- Онлайн-торговля запрещенными товарами
- Домогательства, изготовление или хранение детской порнографии

Киберпреступление всегда подразумевает хотя бы одно из указанного:

- Преступную деятельность с целью *атаки* на компьютеры с использованием вирусов или другого вредоносного ПО.
- *Использование* компьютеров для совершения других преступлений.

Киберпреступники, целью которых является *атака* на компьютеры, могут заражать их вредоносными программами, чтобы повредить или полностью вывести из строя, а также чтобы удалить или похитить данные. Также целью киберпреступников может быть DoS-атака (атака типа «отказ в обслуживании»), из-за которой пользователи или клиенты компании не смогут пользоваться веб-сайтом, компьютерной сетью или программными сервисами.

Киберпреступления, в рамках которых компьютеры *используются* для совершения других преступлений, могут быть нацелены на распространение вредоносного ПО, запрещенной информации или изображений с помощью компьютеров или компьютерных сетей.

Зачастую киберпреступники одновременно и используют, и атакуют компьютеры. Например, они могут сначала атаковать компьютеры с помощью вируса, а затем

использовать их для распространения вредоносного ПО дальше по сети. В некоторых странах классификация киберпреступлений предусматривает еще одну, третью категорию: использование компьютера в качестве вспомогательного средства для совершения преступления. Примером может служить хранение похищенных данных на компьютере.

Примеры киберпреступлений

Ниже приведены нашумевшие примеры различных видов кибератак.

Атаки с использованием вредоносных программ

В этом случае компьютерная система или сеть заражаются компьютерным вирусом или другим вредоносным ПО. После этого киберпреступники могут использовать компьютер для хищения конфиденциальной информации, повреждения данных и других преступных действий.

Известным примером такого рода киберпреступлений является глобальная кибератака, совершенная в мае 2017 г. с помощью программы-вымогателя WannaCry. Такие программы позволяют киберпреступникам требовать выкуп за взятые в «заложники» данные или устройства. WannaCry использовала уязвимость компьютеров под управлением Microsoft Windows.

Тогда от действий программы-вымогателя пострадало 230 000 компьютеров в 150 странах. Жертвы киберпреступников потеряли доступ к своим файлам и получили сообщение с требованием выкупа в биткойнах за восстановление доступа.

Глобальный финансовый ущерб от кибератаки WannaCry оценивается в 4 млрд долларов США. Это киберпреступление до сих пор остается одним из крупнейших по масштабу заражения и ущерба.

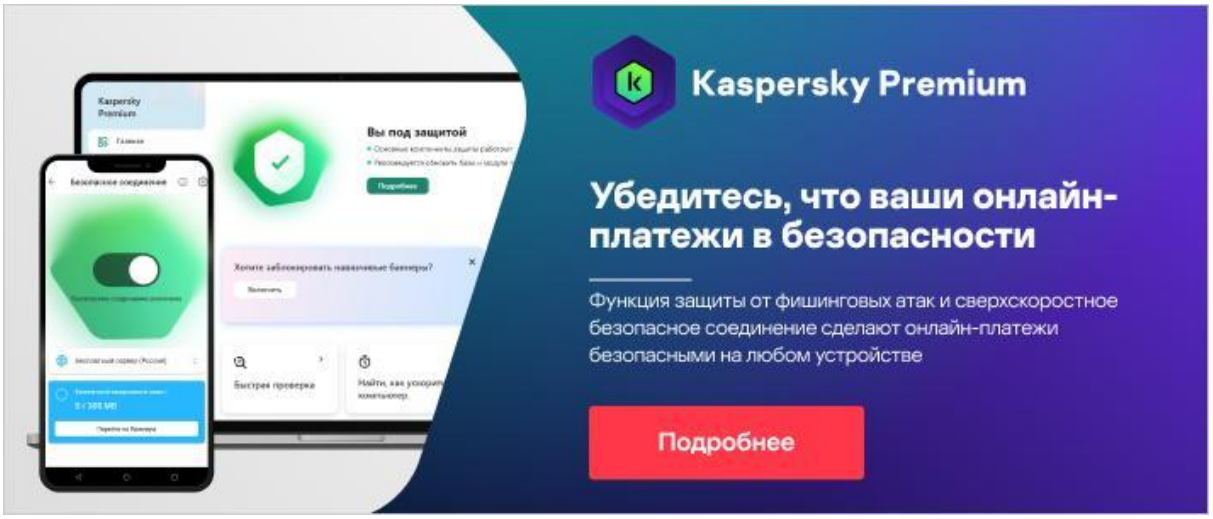
Фишинг

Фишинговая атака – это отправка спама (в электронных письмах или по другим каналам), чтобы обманным путем вынудить пользователей сделать нечто, что ослабит их безопасность. Фишинговые сообщения могут содержать зараженные вложения, ссылки на вредоносные сайты или просьбу предоставить конфиденциальную информацию.

Известный пример фишингового мошенничества произошел в 2018 году во время Чемпионата мира по футболу. Как мы рассказали в отчете «Чемпионат мира по обману 2018», мошенники рассылали футбольным болельщикам фишинговые электронные письма. В качестве приманки авторы спам-рассылки использовали обещание бесплатных билетов в Москву, место проведения Чемпионата мира по футболу 2018 года. У пользователей, которые открывали фишинговые письма и переходили по ссылкам, преступники украли персональные данные.

Еще один вид фишинговой кампании – целевой фишинг. В этом случае киберпреступники организуют направленные фишинговые атаки, чтобы обманным путем вынудить конкретных сотрудников совершить действия, которые нарушат безопасность всей организации.

В отличие от массовых фишинговых рассылок с довольно обобщенным содержанием, письма для целевого фишинга в деталях имитируют сообщения от доверенного источника. Например, может казаться, что письмо отправлено директором или IT-менеджером компании. При этом визуально распознать такое письмо как поддельное может быть очень сложно.



Распределенные DoS-атаки

Распределенные DoS-атаки (DDoS) нацелены на вывод из строя какой-либо системы или сети. Иногда для проведения DDoS-атак используются устройства IoT (интернета вещей).

Отправка множественных запросов на подключение по стандартным протоколам связи в рамках DDoS-атаки приводит к перегрузке системы. Киберпреступники могут угрожать DDoS-атакой в рамках кибершантажа, вымогая деньги. Также DDoS-атака может применяться как отвлекающий маневр во время другого киберпреступления.

Один из громких примеров – DDoS-атака на веб-сайт «Британской национальной лотереи» в 2017 году. Атака полностью нарушила работу веб-сайта и мобильного приложения у лотереи. Мотивы атаки до сих пор неизвестны. Предположительно преступники пытались шантажировать организаторов лотереи.

Последствия киберпреступлений

Количество киберпреступлений продолжает расти. Согласно отчету компании Accenture о состоянии устойчивости к киберугрозам (State of Cybersecurity Resilience) за 2021 г., за период с 2020 по 2021 г. число кибератак выросло на 31%. Число атак в пересчете на одну компанию за год увеличилось с 206 до 270. Атаки на компании затрагивают и обычных людей, так как многие организации хранят у себя конфиденциальную информацию и личные данные своих клиентов и пользователей.

Одна атака, будь то утечка данных, DDoS-атака, заражение программой-вымогателем или другим вредоносным ПО, в среднем обходится компании в 200 000 долларов. А по данным страховой компании Hiscox, многие организации вынуждены полностью прекратить работу в течение полугода после перенесенной кибератаки.

По данным исследования о мошенничестве с кражей цифровой личности, опубликованного в 2021 г. компанией Javelin Strategy & Research, годовой финансовый ущерб от этого вида атак составил 56 млрд долларов.

Таким образом, киберпреступления приводят к серьезным последствиям как для компаний, так и для частных лиц – в основном это финансовый ущерб, а также утрата доверия и репутационные потери.

Защита от киберпреступлений

Учитывая распространенность киберпреступлений, есть ли способ их предотвратить? Вот несколько советов по защите вашего компьютера и персональных данных от киберпреступников.

Регулярное обновление ПО и операционной системы

Регулярное обновление программного обеспечения и операционной системы гарантирует наличие на компьютере актуальных исправлений безопасности.

Использование антивирусных программ и их регулярное обновление

Использование антивирусного или комплексного защитного решения для интернет-безопасности, например Kaspersky Total Security, – хороший способ защитить вашу систему от кибератак. Антивирусные программы позволяют сканировать систему, обнаруживать и нейтрализовать угрозы до того, как они смогут навредить. Качественная антивирусная защита не допустит киберпреступников до компьютера и поможет сохранить ваши данные, пока вы спокойно занимаетесь своими делами. Для полной безопасности регулярно обновляйте антивирусное ПО.

Использование надежных паролей

Устанавливайте надежные пароли, которые никто не сможет подобрать, и не храните их в записанном виде. Также можно использовать проверенный менеджер паролей, который случайным образом сгенерирует надежные пароли за вас.

Привычка не открывать вложенные файлы в письмах

При помощи вложений в спам-письмах киберпреступники реализуют разные виды атак, включая заражение компьютера вредоносными программами. Никогда не открывайте вложенные файлы от неизвестных отправителей.

Привычка не переходить по ссылкам в спам-письмах и на недоверенных веб-сайтах

Люди нередко становятся жертвами киберпреступников, переходя по ссылкам в спам-письмах и других сообщениях, а также на незнакомых веб-сайтах. Чтобы оставаться в безопасности, никогда не переходите по таким ссылкам.

Осторожность при передаче личной информации

Никогда не сообщайте свои персональные данные по телефону или электронной почте, если не до конца уверены в безопасности ваших коммуникаций. Убедитесь, что ваш собеседник действительно тот, за кого себя выдает.

Общение по официальным каналам

Если вам позвонили из организации и в ходе разговора запросили ваши персональные данные, повесьте трубку. Перезвоните по номеру, указанному на официальном веб-сайте компании, чтобы убедиться, что вы разговариваете не с киберпреступником, а с реальным сотрудником. Лучше всего позвонить с другого телефона, так как киберпреступники могут держать прежнюю линию связи открытой. В этом случае вы будете думать, что перезвонили по официальному номеру, тогда как на самом деле продолжите разговаривать со злоумышленниками, которые притворяются представителями банка или другой организации.

Внимательность при посещении веб-сайтов

Обращайте внимание на URL-адреса ссылок, по которым переходите. Убедитесь, что адрес подлинный. Не переходите по ссылкам, URL-адреса которых вам незнакомы или выглядят как спам. Если ваше антивирусное решение поддерживает защиту платежных онлайн-транзакций, убедитесь, что эта функция включена, прежде чем совершать покупку.

Регулярная проверка банковских выписок

Если вы стали жертвой киберпреступления, важно как можно скорее это обнаружить. Регулярно просматривайте историю операций и уточняйте у банка информацию по любым подозрительным транзакциям. Сотрудники банка смогут провести расследование и определить, является ли операция мошеннической.