

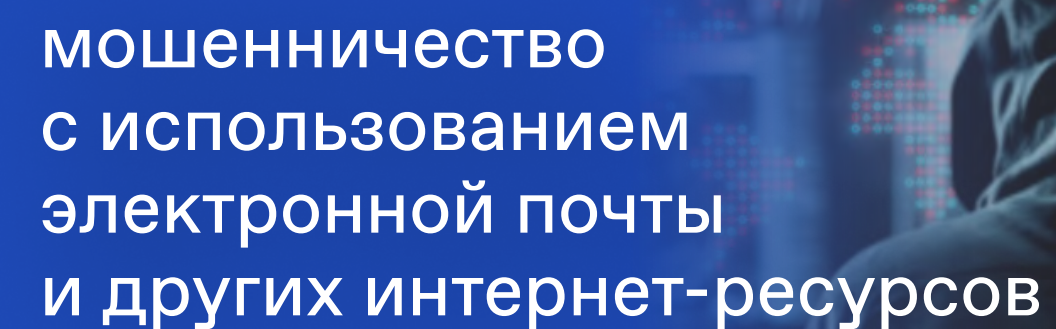
КАК ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИЧЕСТВА: ПРАВИЛА БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

КИБЕРПРЕСТУПНОСТЬ —

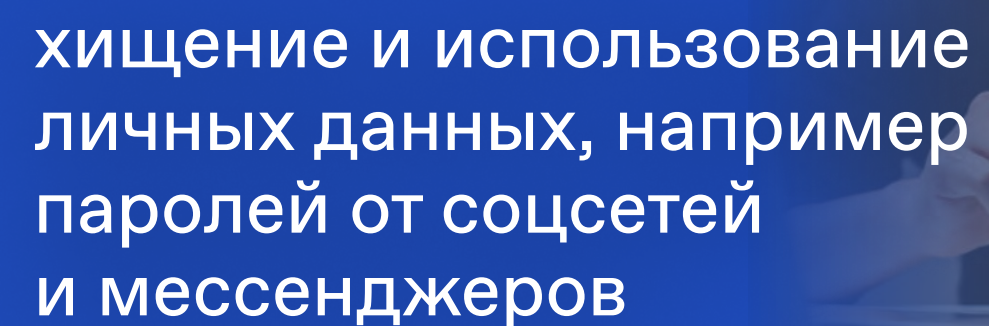


незаконная деятельность, в рамках которой атакуются компьютерные сети, смартфоны и другие устройства для достижения личных, коммерческих или политических целей.

Основные разновидности киберпреступлений:



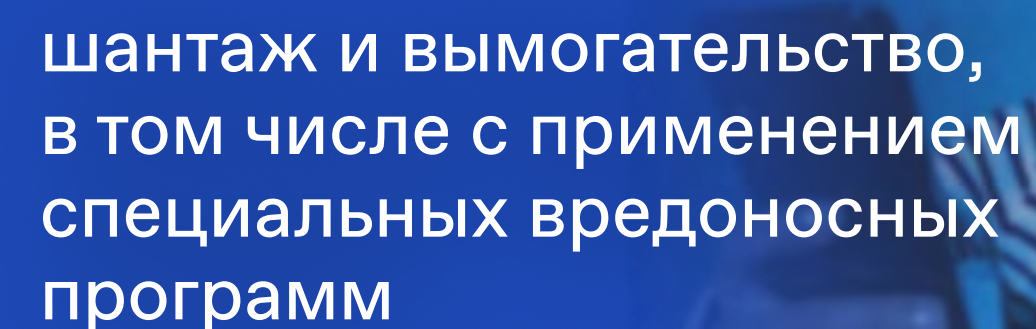
мошенничество с использованием электронной почты и других интернет-ресурсов



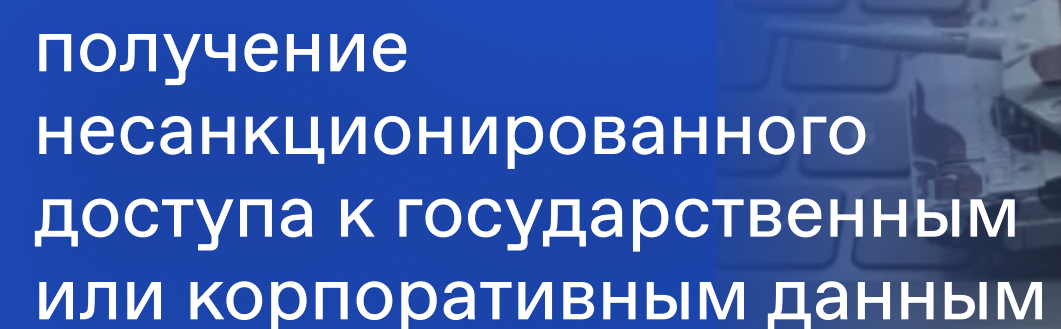
хищение и использование личных данных, например паролей от соцсетей и мессенджеров



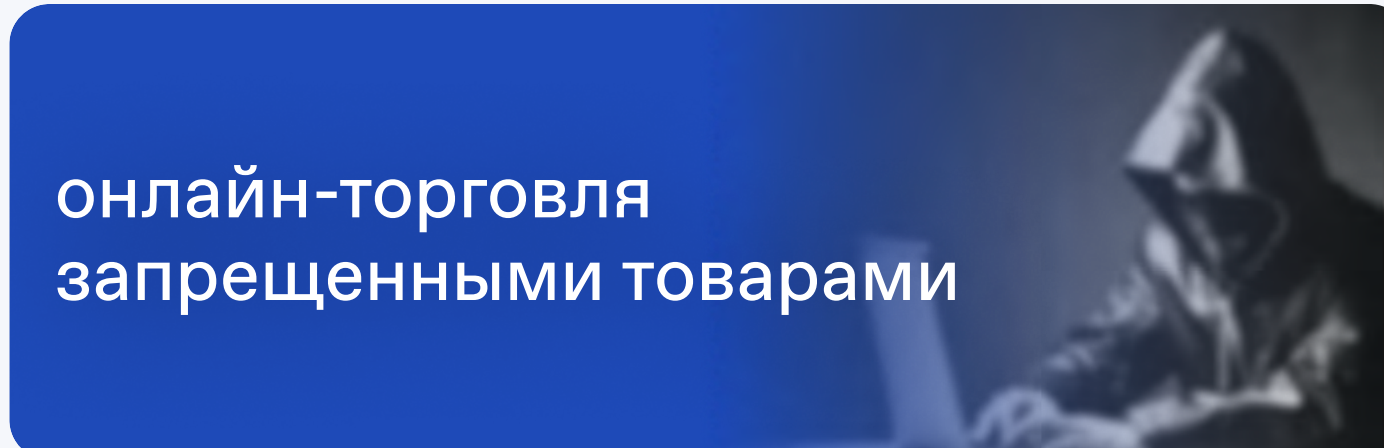
кража данных платежных карт и другой финансовой информации



шантаж и вымогательство, в том числе с применением специальных вредоносных программ



получение несанкционированного доступа к государственным или корпоративным данным



онлайн-торговля запрещенными товарами

СТАТИСТИКА КИБЕРПРЕСТУПНОСТИ



«Кибератаки и факты дистанционной кражи денег у граждан фиксируются чаще, а криминальные схемы, в том числе по выводу незаконно полученных средств, постоянно меняются», — глава МВД России Владимир Колокольцев.

В 2022 году

494 000 киберпреступлений

В 2023 году

более 600 000 киберпреступлений

САМЫЕ РАСПРОСТРАНЕННЫЕ СХЕМЫ МОШЕННИЧЕСТВА



Обзвон граждан от имени правоохранительных органов или банков

Создание фальшивых (фишинговых) сайтов для получения доступа к конфиденциальным данным пользователей

Рассылка писем о «крупном выигрыше» по электронной почте

Фальшивые сайты благотворительных организаций/туроператоров/авиакомпаний

Предложение выгодного заработка на подозрительных интернет-ресурсах

Взлом личных аккаунтов пользователей и рассылка сообщений

Лотереи, викторины, победы в конкурсах, где нужно заплатить «налог на выигрыш» или «комиссию за доставку приза»

НОВЫЕ СХЕМЫ МОШЕННИЧЕСТВА



Дропперы — подставные лица, на которых оформляются банковские карты, куда телефонные мошенники выводят украденные деньги



Создание поддельных Telegram-аккаунтов и имитация голоса близких людей или коллег жертвы с помощью нейросетей



ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ



Если с неизвестного номера звонит сотрудник банка, правоохранительных органов или государственной организации с сомнительным предложением и требует быстрых действий с финансами, положите трубку



Если подозреваете, что вам звонит мошенник, перезвоните в банк или контакт-центр ведомства, сотрудником которого представлялся звонящий



Никому не сообщайте свои паспортные данные и финансовые сведения



Не публикуйте конфиденциальные данные в соцсетях или на сайтах

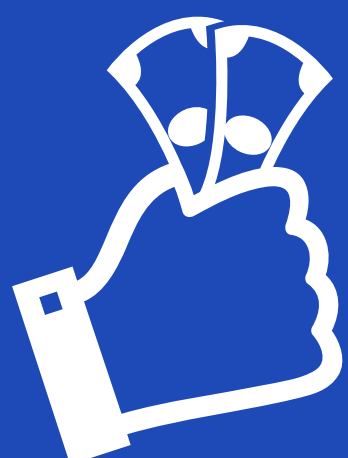


Не храните данные банковских карт и pin-коды на компьютере или в смартфоне

ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ



Защищайте свои аккаунты с помощью двухэтапной аутентификации в тех сервисах, где это возможно



Не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем



Установите антивирус на все устройства и регулярно его обновляйте



Совершайте покупки в интернете только на проверенных сайтах



Не используйте слишком простые пароли и одинаковые пароли для разных учетных записей

НАДЕЖНОСТЬ ПАРОЛЯ И НЕОБХОДИМОЕ ВРЕМЯ ДЛЯ ЕГО ВЗЛОМА



При использовании метода полного перебора (брутфорс)

Количество символов	Только числа	Буквы в нижнем регистре	Буквы в нижнем и верхнем регистре	Числа и буквы в нижнем и верхнем регистре	Числа, буквы в нижнем верхнем регистре, символы
4	мгновенно	мгновенно	мгновенно	мгновенно	мгновенно
5	мгновенно	мгновенно	мгновенно	мгновенно	мгновенно
6	мгновенно	мгновенно	мгновенно	мгновенно	мгновенно
7	мгновенно	мгновенно	2 сек	7 сек	31 сек
8	мгновенно	мгновенно	2 мин	7 мин	39 мин
9	мгновенно	10 сек	1 час	7 часов	2 дня
10	мгновенно	4 мин	3 дня	3 нед	5 мес
11	мгновенно	2 часа	5 мес	3 года	34 года
12	2 сек	2 дня	24 года	200 лет	3 тыс лет
13	19 сек	2 мес	1 тыс лет	12 тыс лет	202 тыс лет
14	3 мин	4 года	64 тыс лет	750 тыс лет	16 млн лет
15	32 мин	100 лет	3 млн лет	46 млн лет	1 блн лет
16	5 часов	3 тыс. лет	173 млн лет	3 блн лет	92 блн лет
17	2 дня	69 тыс. лет	9 блн лет	179 блн лет	7 бллр лет
18	3 недели	2 млн лет	467 блн лет	11 бллр лет	438 бллр лет

ЕСЛИ СРЕДСТВА УЖЕ ПЕРЕВЕДЕНЫ МОШЕННИКАМ



Заблокируйте карту с помощью мобильного приложения, личного кабинета на сайте банка или через контакт-центр банка по телефону



В течение суток после получения сообщения о списании средств напишите заявление в отделение банка о несогласии с операцией



Обратитесь с заявлением о хищении денег в любое отделение полиции



Знание.
Государство

Благодарим
за внимание!



Станем лучше для вас.
Поделитесь впечатлениями!