НИЦМП

Что нужно знать

О КИБЕРБЕЗОПАСНОСТИ?

- СТАТИСТИКА
- ВИДЫ УГРОЗ
- СХЕМЫ ОБМАНА
- КОНТАКТЫ

НИЦМП

СТАТИСТИКА КИБЕРПРЕСТУПЛЕНИЙ В РОССИИ

В **январе–августе 2024** года зарегистрировано **500,4 тысячи преступлений**, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что **на 16,4% больше, чем январе–августе 2023 года.**

В настоящее время **доля киберпреступлений** в общем массиве составляет около **40%** – то есть **почти каждое второе преступление.**

В России ущерб от киберпреступлений превысил **116 млрд руб. с начала 2024 г.**

Информация подготовлена по данным МВД России

НАИБОЛЕЕ ЭФФЕКТИВНЫЙ МЕТОД ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ – ЗНАНИЕ СХЕМ СОВЕРШЕНИЯ И СПОСОБОВ ЗАЩИТЫ ОТ НИХ.

НИЦМП

КАКИЕ СУЩЕСТВУЮТ ВИДЫ КИБЕРУГРОЗ?

Киберпреступление – действия, организованные одним или несколькими злоумышленниками, направленные на кражу данных, обман частных лиц и предприятий, сбой работы сервисов. Главная цель – извлечь финансовую выгоду.

Кибератака – действия, нацеленные на информационную систему с целью попытки получить несанкционированный доступ к компьютерным системам и украсть, изменить или уничтожить данные.

Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику у населения или конкретных ее представителей.

Кибербезопасность – это деятельность, включающая совокупность методов и приемов, по защите компьютеров, серверов, мобильных устройств, приложений, электронных систем и интернет-сетей от действий злоумышленников.

НИЦМП

КАКИЕ ОСНОВНЫЕ СХЕМЫ ОБМАНА?

- **Звонок из банка или правоохранительных органов** с информацией о попытке взлома банковского счета, аккаунта госуслуг и т.д.
- **Звонок, текстовое или голосовое сообщение якобы от руководителя вашей организации** по факту якобы взаимодействия с правоохранительными органами и с целью обеспечения сохранности денежных средств.
- Текстовые или голосовые сообщения, звонок **якобы от родственника или знакомого с просьбой о срочной помощи.**
- **Сообщения с просьбой пройти по ссылке** (проголосовать, посмотреть какую-либо информацию и т.д.).
- **Сообщения с кодом подтверждения,** который нужно ввести, но вы его не запрашивали.
- **Навязчивые звонки с неизвестных номеров** (перезвонив на них, с вашей сим-карты спишут деньги!).

! **Увеличение числа киберпреступлений связано с ростом технических возможностей, в частности, доступностью искусственного интеллекта, а также с привлекательностью цифровой среды за счет факторов ее анонимности и трансграничности.**

НИЦМП

ПРАВИЛО ТРЕХ «НЕ» В ПРОТИВОДЕЙСТВИИ КИБЕРУГРОЗАМ

НЕ ВЕРЬТЕ И НЕ ПАНИКУЙТЕ
Любой звонок или сообщение о финансовых вопросах (как хищение средств, так и предложения получения прибыли), просьбах раскрыть личные данные, угрозах, шантаже и иные действия стоит воспринимать как акт мошенничества!

НЕ ПРОДОЛЖАЙТЕ ТЕЛЕФОННЫЙ РАЗГОВОР, НЕ ВСТУПАЙТЕ В ПЕРЕПИСКУ
Даже если вы уверены в себе, что не попадетесь на уловки злоумышленника, общаться не стоит. Киберпреступники используют механизмы психологического воздействия такие как внушение, убеждение, побуждение, поэтому риск есть всегда.

НЕ СОВЕРШАЙТЕ КАКИЕ-ЛИБО ДЕЙСТВИЯ
Не сообщайте никакие данные, не переводите никуда деньги, не берите кредиты, не пишите и не отправляйте какие-либо заявления или иные документы по требованию.

НИЦМП

КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ?

ЕСЛИ ОПАСНОСТЬ УГРОЖАЕТ ПРЯМО СЕЙЧАС

- Единый номер вызова экстренных оперативных служб **112.**

ЕСЛИ ЕСТЬ ПОДОЗРЕНИЯ ОБ АКТАХ МОШЕННИЧЕСТВА ИЛИ НУЖНА КОНСУЛЬТАЦИЯ

- Виртуальная горячая линия по проблемам кибербезопасности **http://resurs-center.ru/hotline.**
- Горячая линия «Кибербезопасность» от НИЦ Мониторинга и профилактики **https://vk.com/nicmp.**

ЕСЛИ ОТ ИМЕНИ БАНКА ЗАПРАШИВАЮТ ПЕРСОНАЛЬНЫЕ СВЕДЕНИЯ, ДАННЫЕ БАНКОВСКИХ КАРТ, ПРЕДЛАГАЮТ СОВЕРШИТЬ КАКИЕ-ЛИБО ОПЕРАЦИИ

- Горячая линия Центробанка РФ для физических лиц телефон для обращений **8 800 300 30 00.**