**Анализ преступлений по потерпевшим за 2023г.**

**Количество киберпреступлений в 2023 году выросло почти на 30%**

За 5 месяцев 2023 года в России выявлено 261 тысяча киберпреступлений.

Фото: Arnold Francisca / unsplash

МВД [опубликовало](https://www.pnp.ru/social/chislo-kiberprestupleniy-v-rossii-v-yanvare-mae-vyroslo-pochti-na-28.html) отчёт о состоянии преступности в стране, где указывается на рост количества киберпреступлений в 2023 году и его распределение по регионам. Лидером по приросту преступлений в информационной среде стала Ингушетия, а в Чечне этот показатель упал более чем на 50%.

За период январь-май 2023 года министерство выявило 261 тысячу киберпреступлений, что на 27,5% больше, чем за тот же период 2022 года. Основная часть преступлений совершается через интернет, а также киберпреступники стали чаще использовать мобильные средства связи. Случаи мошенничества с электронными средствами платежа при этом сократились на 32%.

Ингушетия стала лидером по приросту преступлений с использованием информационных технологий (+217%), на втором месте Ненецкий АО (+215%), рост от 57% до 90% зафиксирован в Томской, Ярославской, Липецкой, Новгородской, Белгородской и Тульской областях, а также в Мордовии и Ямало-Ненецком АО.

Есть регионы и с положительными изменениями. Так в Чечне количество киберпреступлений снизилось на 52,9%, в Дагестане на 23%, а в Подмосковье на 0,3%.

На данный момент в России активно ведётся борьба с киберпреступностью на всех уровнях: от административной и уголовной ответственности за утечки информации до принудительной блокировки счетов подозреваемых в мошенничестве.

1 августа 2023, 10:07

# В России число совершенных через мобильную связь и интернет преступлений выросло на 39%

### В Генпрокуратуре в январе-июне 2023 года зарегистрировали более 210,8 тыс. различных мошенничеств

МОСКВА, 1 августа. /ТАСС/. Число преступлений, совершенных с использованием сети Интернет и средств мобильной связи, выросло в 2023 году на 39,3% по сравнению с аналогичным периодом прошлого года. Об этом ТАСС сообщили в пресс-службе Генпрокуратуры, отвечая на запрос агентства.

"В январе-июне 2023 года зарегистрировано более 210,8 тыс. различных мошенничеств, - сообщили в пресс-службе надзорного ведомства со ссылкой на данные правовой статистики. - В структуре подобного рода хищений значительна доля (79,1%) мошенничеств, совершенных дистанционно, с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (166,8 тыс.). Темп их прироста относительно первого полугодия прошлого года увеличился на 40,5%".

При этом количество мошенничеств с использованием электронных средств платежа (когда с помощью скрининга платежных карт или путем обмана мошенники получают данные банковских карт) сократился более чем на треть (до 2,9 тыс.).

## Кражи и мошенничества

Как отметили в Генпрокуратуре, более половины выявленных за полугодие преступлений против собственности совершено путем кражи. Их массив уменьшился на 17,6% (до 284,1 тыс.). Число краж с банковского счета в сравнении с аналогичным периодом прошлого года осталось практически на прежнем уровне (56,2 тыс.).

Общее число зарегистрированных мошенничеств (ст. 159-159.6 УК РФ) выросло в стране за полгода почти на треть. "Их доля в структуре преступности на протяжении последних лет последовательно увеличивается и составляет 21,4%", - сообщили в Генпрокуратуре.

При этом, если раскрываемость краж составляет 48%, то раскрываемость мошенничеств - 22,8%. Так, в ЦФО за полгода раскрыто 25,8% мошенничеств, в СЗФО - 17,1%, в СКФО - 37,5%, в ЮФО - 26,5%, в Приволжском федеральном округе - 19,6%, в Уральском - 23,4%, Сибирском - 18,1%, Дальневосточном - 17,2%. В Москве за полгода раскрыто 27,6% мошенничеств, в Подмосковье - 35,9%, в Санкт-Петербурге - 13,5%. В Краснодарском крае раскрыто 22,4% мошенничеств, в Новосибирской области - 19,3%, в Свердловской - 18,5%, Красноярском крае - 17,4%, Приморском крае - 13,7%. Самые высокие показатели раскрываемости мошенничеств - в Чечне (84,3%) и Дагестане (71,6%), самые низкие - в Смоленской (8,1%) и Тверской (7,2%) областях.

# Опасная реклама: как не стать жертвой хакеров, кликнув на баннер

Всплывающие окна с рекламой являются неотъемлемой частью нашей жизни. Пользователи с их помощью могут находить нужные товары и услуги, а разработчики на этом зарабатывают, продавая рекламные места. Вот только покупатели не всегда бывают добросовестными, всплывающее окно может содержать много опасностей. Как злоумышленники используют pop-up в реальных атаках и как защититься от такого вида хакинга – в материале «Инфобезопасности».

## Что такое поп-ап окна и зачем они нужны?

Поп-ап окна, они же всплывающая реклама, нужны для быстрого показа пользователю какой-либо информации. Это может быть уведомление, предложение или реклама. С их помощью пользователя предупреждают о сборе куки-файлов, предлагают подписаться на рассылку или рекламируют продукт.

Такое предложение пользователь может принять, либо отказаться от него, нажав на крестик. А ещё они обычно закрывают часть контента, чтобы на них точно обратили внимание.

Возможность использования таких окон пришла вместе со стандартом web2, когда сайты стали информативными. Для появления поп-ап окна требуется какое-либо действие посетителя сайта, только тогда срабатывает код и пользователь видит контент.

В большинстве своём поп-ап окна не несут никакого вреда, кроме того, что они назойливы, закрывают контент и иногда не закрываются с первого раза.

## Когда поп-ап окна могут оказаться опасными?

Реклама во всплывающих окнах, как и любая другая реклама, продаётся. Такой баннер для своей услуги может купить как порядочный разработчик новой игры, так и хакерская группировка. И только во втором случае баннер будет нести серьезную опасность.

Злоумышленники могут встроить вредоносный код во всплывающее окно и реализовать один из трёх сценариев:

1. Фишинг. Ссылка из рекламы может вести на фейковый сайт, где расположена поддельная форма для ввода данных или загрузки вредоносного ПО.
2. Заражение устройства. Клик по всплывающей рекламе может вызвать автоматическую загрузку софта на устройства и пользователь даже не заметит, как его устройства окажется заражено майнером, стилером или программой-вымогателем.
3. Браузерные зловреды. «Крестик» для закрытия рекламы может не выполнять своих функций, а наоборот открывать дополнительное окно, содержащее неприемлемый контент или еще больше рекламы.

## Меры борьбы с опасной рекламой

Современные браузеры позволяют отключать всплывающие окна на сайтах. Кроме того, многие из них делают это автоматически, если обнаружена подозрительная активность. Однако, запрет на показ поп-ап окон не всегда полезен, так как может препятствовать нормальной работоспособности сайта и даже закрыть вам доступ к важным функциям.

Наиболее эффективно с назойливыми и даже вредоносными рекламными окнами справляются блокировщики рекламы. Но их нужно устанавливать только из официальных источников.

Также полезным будет использование антивирусного ПО, которое способно сразу обнаружить угрозу и предотвратить его. А ещё сохранение бдительности, отказ от переходов по сомнительным ссылкам и регулярное обновление ОС и приложений для получения свежих апдейтов.

## Заключение

Поп-ап окна могут быть не только навязчивыми и раздражать пользователей, но крайне опасными. Злоумышленники с помощью всплывающей рекламы могу проводить фишинговые атаки, заражать устройство вредоносным ПО или даже отслеживать вашу активность в сети.

Чтобы не стать жертвой рекламы, лучше сразу принять меры для устранения таких сценариев. Например, установить на все устройства антивирусное ПО, использовать блокировщики рекламы и всегда сохранять бдительность.