КУДА СООБЩАТЬ О МОШЕННИЧЕСТВЕ В ИНТЕРНЕТЕ:

- в службу технической поддержки банка или платежной системы, осуществляющей переводы денежных средств, чтобы заблокировать счет;
- в полицию по месту проживания;
- в Роскомнадзор, осуществляющий контроль за деятельностью организаций по оказанию услуг в области электронных технологий.

ЕСЛИ У МОШЕННИКОВ ЕСТЬ ВРЕДОНОСНЫЙ САЙТ, ТО СООБЩИТЬ О НЕМ ДЛЯ ОПЕРАТИВНОЙ БЛОКИРОВКИ МОЖНО В СЛУЖБУ ПОДДЕРЖКИ ЯНДЕКС, ГУГЛ ИЛИ Т. П. ПРИ ПРЕДОСТАВЛЕНИИ УБЕДИТЕЛЬНЫХ ДОКАЗАТЕЛЬСТВ САЙТ ЗАБЛОКИРУЮТ.

ПРОКУРАТУРА РАЗЪЯСНЯЕТ

ВИДЫ И СХЕМЫ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НЕ ТОЛЬКО ОТКРЫВАЕТ НОВЫЕ ВОЗМОЖНОСТИ ОБЩЕСТВУ, НО И ВООРУЖАЕТ ПРЕСТУПНИКОВ НОВЫМИ СПОСОБАМИ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ

МОШЕННИЧЕСТВО - ЭТО ХИЩЕНИЕ ЧУЖОГО ИМУЩЕСТВА ИЛИ ПРИОБРЕТЕНИЕ ПРАВА НА ЧУЖОЕ ИМУЩЕСТВО ПУТЕМ ОБМАНА ИЛИ ЗЛОУПОТРЕБЛЕНИЯ ДОВЕРИЕМ, ЧТО ЯВЛЯЕТСЯ ПРЕСТУПЛЕНИЕМ В СООТВЕТСТВИИ СО СТ. **159** УК РФ.

In the United States as well as the other parts of the globe, professional licenses are required by agencies in order for them to hire the MUA. Bigger production companies have in-house makeup artists on their payroll although most MUA's generally are freelance and their times remain flexible depending on the projects.

ПОПУЛЯРНЫЕ ВИДЫ ИНТЕРНЕТ-МОШЕННИЧЕСТВА:

ФИШИНГ -
кража идентификационных данных (например, ФИО, пароль и номер банковской карты). Злоумышленники пользуются невнимательностью граждан и завладевают конфиденциальной информацией путем создания сайтов-клонов, фальшивых аккаунтов в мессенджерах и соцсетях, электронной рассылки писем. Преступники выдают себя за надежный источник в сети, вынуждая жертву передать им личные данные.

КАРДИНГ -
тип интернет-преступлений, при котором мошенники обманным путем совершают кражу конфиденциальной информации о пользователях и снимают деньги со счетов граждан без их ведома. Самый распространенный способ получения доступа к данным банковских карт — взлом серверов интернет-магазинов, расчетных и платежных систем. Хакеры используют программы удаленного доступа и вредоносное ПО (программное обеспечение) для получения персональной информации о человеке и данных о платежной карте.

САМЫЕ РАСПРОСТРАНЕННЫЕ СХЕМЫ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ В КИБЕРПРОСТРАНСТВЕ:

Двойники интернет-магазинов
Через поисковые системы пользователи переходят по ссылке, проходят регистрацию и вводят информацию о своем банковском счете для завершения покупки. В итоге продавец получает оплату и пропадает или присылает совершенно иной товар. Нужно всегда проверять адресную строку в браузере. Она должна начинаться с "https" (безопасный протокол передачи данных), это означает, что ресурс имеет защищенное (шифрованное) соединение, хотя и не гарантирует полной безопасности.

Копии сервисов интернет-банкинга
Злоумышленники создают сайты-клоны банков. Посредством электронного письма или смс-сообщения приглашают пользователей пройти авторизацию. Граждане переходят на фальшивый сайт, регистрируются в личном кабинете, раскрывая логин и пароль для доступа к финансам.

Фишинговая атака по электронной почте Рассылка писем с сообщением о выигранном призе или о блокировке счета. Преступники, как правило, просят победителя перевести определенную сумму для получения крупного выигрыша или внести оплату для разблокировки карты.