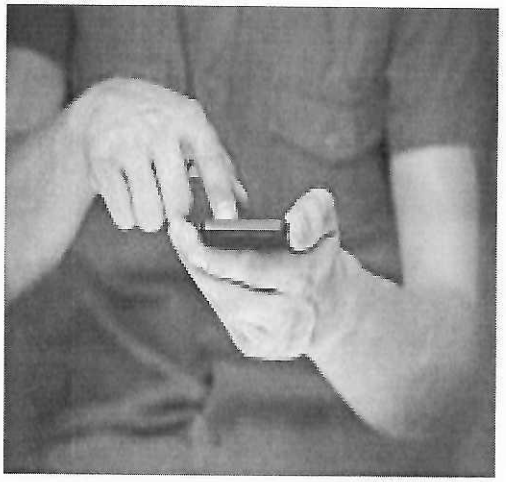
Не устанавливайте приложения на свои смартфоны!



01.11.2022 года в МУ МВД России по ЗАТО г. Саров обратился гражданин «Д» с заявлением о том, что с его банковской карты незаконно были списаны денежные средства в сумме 21000 рублей при следующих обстоятельствах: на его номер телефона поступил звонок, мужчина представился сотрудником службы безопасности Сбербанка. В ходе телефонного разговора последний сообщил, что зафиксирована «ненормальная» активность его банковской карты. Гражданин «Д» не поверил, ведь его карта находится при нем, а значит ей никто не пользуется. Сотрудник банка поспешил сказать, что это не важно, карту нужно заблокировать, а для этого гражданину «Д» необходимо зайти в «Плей Маркет», в поисковой строке найти приложение «AirDroid Cast-screen mirroring» и установить его к себе на телефон. После установки, гражданин «Д» по просьбе сотрудника Сбербанка запустил трансляцию на своем мобильном телефоне с помощью установленного приложения. В результате, мошенник получил удаленный доступ к телефону гражданина «Д» с помощью чего произвел манипуляции, которые позволили списать с его карты 21000 рублей.

По данному факту возбужденно уголовное дело, проводится проверка.

Никогда не предоставляйте незнакомым лицам доступ к своим устройствам и не скачивайте никакие приложения на свой гаджет!

21.01.2023 в МУ МВД России по ЗАТО г. Саров обратился гражданин «Д» с заявлением в котором указал, что на его мобильный номер телефона поступил звонок, молодой человек представился помощником сотрудника ФСБ и предложил поучаствовать в поимке мошенников. С его слов, скоро в Саров приедут люди, которые хотят приобрести его автомобиль «Toyota Hailuxe». От него требовалось заключить договор купли-продажи, по которому получить деньги. По имеющейся информации, купюры будут фальшивые. Также молодой человек сообщил, что в Сарове есть два банкомата которые могут «отделять» фальшивые деньги от настоящих. Ему необходимо будет внести денежные средства на счет, после чего фальшивые купюры – отсеются, а настоящие поступят на счет ФСБ. Гражданин «Д» согласился помочь. Спустя некоторое время ему поступил телефонный звонок от покупателя. В ходе телефонного разговора, была достигнута договоренность о встрече. В назначенное время, гражданин «Д» выехал за 3 КПП г. Саров где ждали его покупатели. Между ними был заключен договор купли-продажи, предметом которого являлся автомобиль «Toyota Hailuxe» 2012 г.в., цена договора – 700 000 рублей. После того как гражданин «Д» получил вышеуказанную сумму, а покупатели автомобиль, он сразу же направился в отделение ПАО «Сбербанк», расположенное по адресу: г. Саров, ул. Зернова, д. 34 и при помощи банкомата, перевел 700 000 рублей на указанный помощником сотрудника ФСБ банковский счет.

По данному факту возбуждено уголовное дело.

31.02.2023 в МУ МВД России по ЗАТО г. Саров обратилась гражданка «М.» сообщив, что стала жертвой мошенников. По словам потерпевшей, на сайте XX.RU она обнаружила объявление о работе, которое ее заинтересовало. Она составила свое резюме, где указала контактный номер телефона. В этот же день, в мессенджере «WhatsApp» ей пришло сообщение с неизвестного номера, в котором говорилось о легком заработке. Суть его заключалась в том, что ей необходимо будет вносить денежные средства на определенные счета, с которых в последующем осуществлять покупку товаров из предложенного списка в магазине «Wildberries». С каждой покупки гражданке «М» полагался приятный бонус в виде денежных средств в размере 40% (от стоимости покупки). В предвкушении легкого заработка, действуя по указанию мошенников, гражданка «М» перевела 86 066 рублей со счетов своих банковских карт по реквизитам, предоставленным ей «работодателем»

По данному факту возбуждено уголовное дело.

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг — вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций

КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, объявлений о лотереях, распродажах, компенсациях от государства

! **Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых**

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- **Адрес** отличается от настоящего лишь парой символов
- **В адресной строке** нет https и значка закрытого замка
- **Дизайн** скопирован некачественно, в текстах есть ошибки
- **У сайта** мало страниц или даже одна — для ввода данных карты

КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- **Установите** антивирус и регулярно обновляйте его
- **Сохраняйте** в закладках адреса нужных сайтов
- **Не переходите** по подозрительным ссылкам
- **Используйте** отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой

Подробнее о правилах кибергигиены читайте на fincult.info

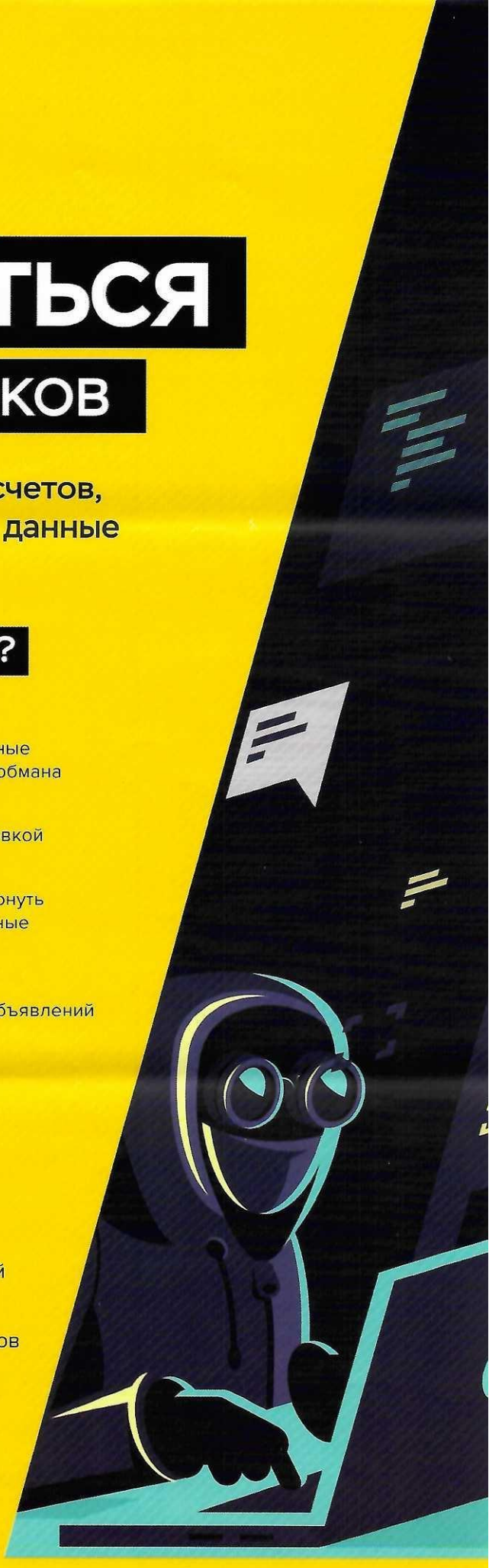
Финансовая культура

ГУ МВД России по Нижегородской области

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт



Какие схемы используют аферисты?

ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ
Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

ЗАМАНИВАЮТ НА РАСПРОДАЖИ
Огромные скидки и низкие цены могут оказаться мошеннической уловкой

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ
Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

МАСКИРУЮТСЯ
Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений

Как обезопасить свои деньги в интернете?

1. Установите антивирус и регулярно обновляйте его
2. Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
3. Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
4. Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
5. Никому не сообщайте свои персональные данные

Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

ГУ МВД России по Нижегородской области