Памятка по информационной безопасности

📱 Когда человек под воздействием мошенников скомпрометировал свои учетные записи, устройства или аккаунты в онлайн-сервисах, у него есть «золотой час», как и для экстренной помощи в медицине, чтобы минимизировать последствия.

❗ Если вы только что сообщили аферистам данные банковской карты, то необходимо предпринять следующие шаги:

➖ оперативно сменить пароль, код доступа в банковский сервис;

➖ заморозить банковские карты и счета.

💳⚫ Незамедлительно свяжитесь с банком по номеру, указанному на банковской карте или официальном сайте, сообщите о звонке или сообщении злоумышленников и продиктуйте телефонный номер, который они использовали.

Предупредите родных, близких, работодателя, что ваши банковские карты могут быть скомпрометированы и лучше не переводить на них деньги. 📲

❗ Если атаке подверглась ваша учетная запись на популярном государственном сервисе, то следует оперативно сменить пароль, код доступа, позвонить на горячую линию сервиса и сообщить о произошедшем.

Если вы отреагировали своевременно и еще не потеряли возможность войти в личный кабинет – проверьте заявки, разрешения, в том числе в сторонних сервисах.

🆘 Обязательно обратитесь в МВД России и передайте всю информацию об инциденте ❗

❗ Если вы заподозрили, что ваш мобильный номер оказался под контролем третьих лиц, – свяжитесь с вашим оператором по официальному номеру телефона, в приложении или в салоне связи и сообщите об этом.

📞 Порядок действий может немного отличаться в зависимости от вашего оператора. Однако в любом случае стоит привязать сервисы, соцсети, мессенджеры к нескомпрометированному номеру телефона.

Внимательно следите за приходящими СМС о блокировке, перевыпуске или переносе сим-карт.

Предупредите родных, друзей, коллег, что с вашего номера могут звонить или писать злоумышленники с просьбой одолжить денег или поделиться чувствительной информацией.

❗ Мошенники могут использовать также мессенджеры и соцсети, чтобы получить доступ к личной информации, шантажировать вас или для проведения дальнейших сложных криминальных схем. Если вы подозреваете, что учетная запись скомпрометирована (например, не приходят одноразовые коды безопасности), то следует сразу обратиться в службу поддержки. Кроме того, смените пароль на совершенно новый и достаточно сложный, включите двухфакторную идентификацию.

✔️ В списке привязанных к аккаунту устройств срочно отключите все незнакомые и недоступные вам девайсы.

🤝 Предупредите ваш круг контактов, что через ваш аккаунт в мессенджере злоумышленники могут рассылать сообщения с просьбой одолжить денег. 💸

🚨🚨🚨🚨🚨🚨🚨🚨🚨

❗📢 Все эти риски можно свести к минимуму, если заблаговременно соблюдать правила цифровой гигиены, настроить все доступные инструменты безопасности в сервисах, не переходить по подозрительным ссылкам, не открывать сомнительные файлы и не сообщать посторонним персональную информацию и коды.