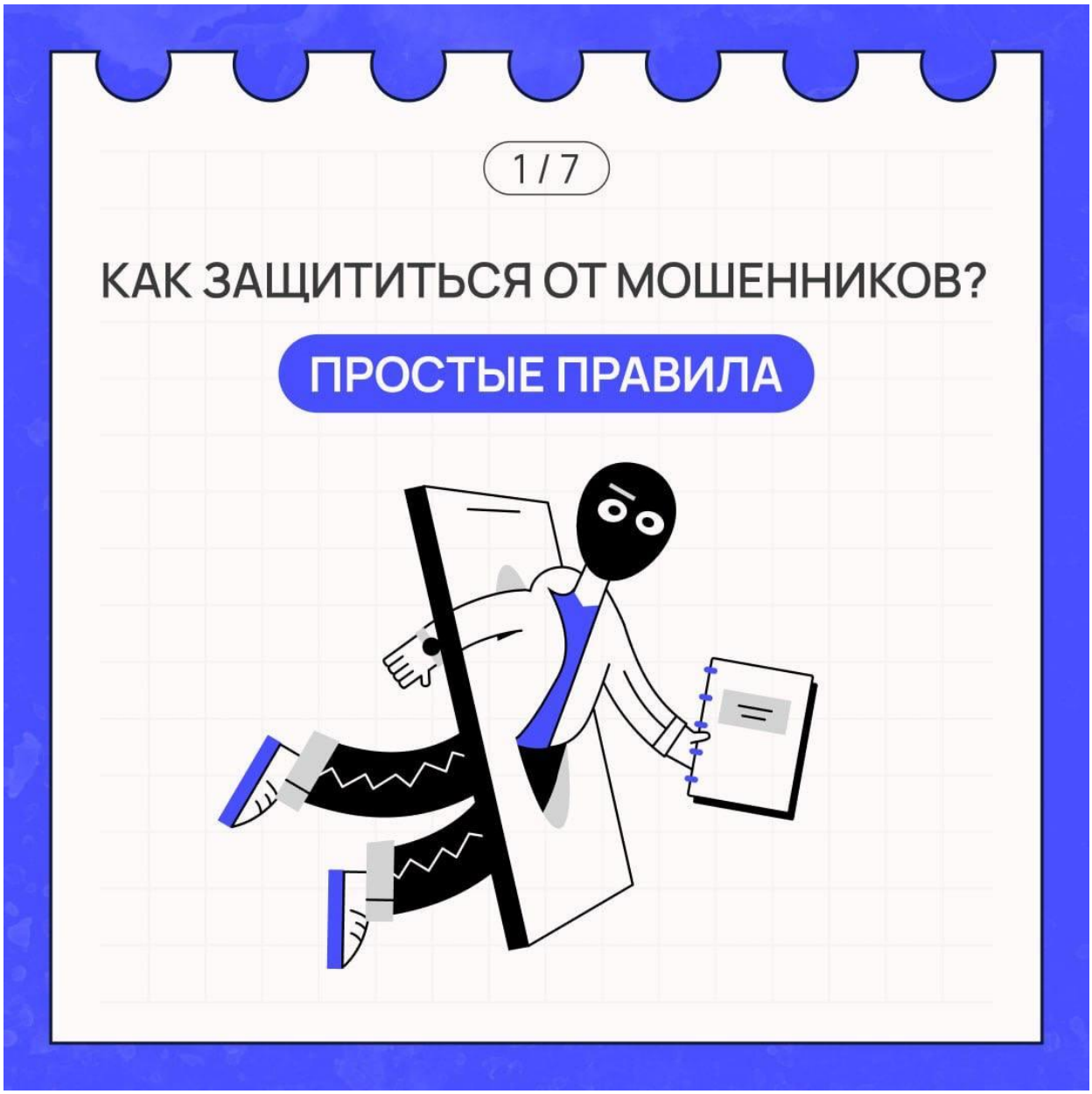
Как защитить себя от утечек данных в сети?

Все мы пользуемся электронными устройствами, оплачиваем покупки в онлайн-сервисах и имеем странички в социальных сетях. Благодаря этому становятся доступными такие данные, как ФИО, электронная почта, номер телефона. К сожалению, мошенники не дремлют и ищут способ нажиться на чем угодно. Для проворачивания преступных схем они используют даже такой скудный набор информации.

Ежемесячно в лентах появляются новости о том, что у крупной компании были «слиты» базы данных клиентов или украдены деньги со счетов обычных граждан.

Как защитить себя в интернете? Рассказываем в карточках.



ТО, ЧТО НУЖНО ЗНАТЬ

- Будьте бдительны! Если разговор кажется подозрительным, завершите его и перезвоните в организацию по официальным номерам;
- Проверяйте способ связи. Мошенники часто используют мессенджеры, такие как WhatsApp или Telegram;
- Не сообщайте логины и пароли, а также не делитесь ответами на контрольные вопросы.

ТО, ЧТО НУЖНО ЗНАТЬ

- Следите за актуальностью номера. Убедитесь, что номер, к которому привязан аккаунт, все еще в вашем распоряжении;
- Используйте сложные пароли. Регулярно меняйте их и подключите двухфакторную аутентификацию;
- Проверяйте адрес страницы. Убедитесь, что сайт — это официальный ресурс.

ВНИМАНИЕ!

Мошенники также часто используют электронную почту и мессенджеры для своих афер. При получении подозрительных писем обратите внимание:

- Знаком ли вам отправитель?
- Присутствуют ли URL-ссылки?
- Есть ли вложение с расширениями .zip, .js, .exe?
- Просит ли файл включить поддержку макросов?

Если письмо вызывает подозрения,
то велика вероятность, что это фишинг.

МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

- Проверяйте адреса электронной почты отправителя, даже если имя совпадает с известным контактом;
- Не открывайте письма и чаты от неизвестных отправителей. Если случайно открыли, то ни в коем случае не переходите по ссылкам в письме;
- Не подключайте неизвестные внешние носители информации к компьютерам;

МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

- Используйте надежные менеджеры паролей для их хранения и управления;
- Используйте надежные пароли, создавайте их с нестандартными комбинациями символов и регулярно меняйте;
- Не используйте один и тот же пароль для разных учетных записей. Создавайте уникальные пароли для каждой важной учетной записи;

ГДЕ ЕЩЕ МОЖНО НАЙТИ ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ ПО ТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

В разделе «Кибербезопасность — это просто!» на Едином портале государственных услуг

На лендинговой странице сайта киберзож.рф