ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

• Использование антивирусного программного обеспечения, а также своевременное обновление его баз.

• Регулярное полное сканирование информационных систем средствами антивирусной защиты.

• Выполнение всех рекомендаций по работе с вложениями, пришедшими из подозрительных источников, в том числе рекомендаций не открывать вложения — исполняемые файлы и не включать макросы в документах Microsoft Office, если нет уверенности в надежности отправителя.

• Отказ в подтверждении вызывающих сомнение платежей до выяснения всех обстоятельств.

• Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам.

Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках.

• Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление финансовой организации), а затем поступает звонок от лица, который по ошибке зачислил вам деньги и просит вернуть, не спешите их переводить.

Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС — не от вашей финансовой организации, а звонил вам злоумышленник. Проверьте состояние вашего счета, закажите выписку, позвоните в финансовую организацию, прежде чем переводить кому-то деньги.

• Никому не сообщайте персональные данные, пароли и коды. Сотрудникам финансовой организации они не нужны, а мошенникам откроют доступ к вашим средствам.

• При получении первичного пароля для входа в Личный кабинет финансовой организации изменяйте его на личный.

• Не храните данные карт на компьютере или в смартфоне.

• Проверяйте информацию. Если вам говорят, будто вы что-то выиграли или с вашей карты случайно списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в финансовую организацию.

• Если вам поступает звонок якобы от службы безопасности финансовой организации, в которой вы обслуживаетесь, с информацией о том, что кто-то пытается с использованием ваших персональных данных взять кредит (заем) или осуществить несанкционированную операцию с вашего счета, не спешите следовать инструкциям злоумышленника.

Положите трубку, перезвоните в финансовую организацию и уточните полученную информацию.