ДЛЯ УЧИТЕЛЯ

Кейс № 1

1 СИТУАЦИЯ

В кафе официант приносит вам POS-терминал, вы расплачиваетесь, но тут официант говорит, что оплата не прошла, и просит повторно ввести ПИН-код вашей карты. Ваши действия?

ЭКСПЕРТ

Вводя повторно ПИН-код, вы рискуете заплатить дважды. Подключите СМС- или push-уведомления о платежах по вашей карте. Обязательно попросите чек с уведомлением о сбое или отказе от операции (POS-терминал всегда печатает такой).

---

2 СИТУАЦИЯ

После поездки в переполненном автобусе вы не смогли обнаружить кошелек в своем рюкзаке. Очевидно, что его у вас украли. В кошельке были не только деньги, но и карта, на которую вам перечисляют стипендию. Ваши действия?

ЭКСПЕРТ

Необходимо позвонить в банк и заблокировать карту. Если вы не можете связаться с банком по телефону, зайдите в ближайшее отделение банка и напишите заявление о блокировке. Также вы можете заблокировать карту через онлайн-банк.

---

3 СИТУАЦИЯ

Вы хотите продать свой старый телефон через сайт объявлений в интернете. С вами связался заинтересованный покупатель и готов перевести деньги вам на карту. Он просит вас сообщить номер карты, срок действия, имя держателя на английском языке, а также трехзначный код на оборотной стороне карты. Так деньги точно дойдут. Ваши действия?

ЭКСПЕРТ

Такой подход должен вас насторожить — для перевода денег достаточно знать только номер карты. Если вы передадите основные платежные данные карты, то рискуете остаться без денег. Мошенники смогут расплатиться картой в интернет-магазине.

---

4 СИТУАЦИЯ

На интернет-сайте, посвященном новинкам в области мобильных гаджетов, вы увидели программу, позволяющую бесплатно звонить друзьям. Ее можно скачать на ваш телефон. Вы впервые на данном сай-

те, предложение скачать программу весьма заманчиво, с таким вы еще не сталкивались. Ваши действия?

ЭКСПЕРТ

Скачав программу, вы рискуете заразить вирусом свой компьютер. Для скачивания программ используйте только проверенные интернет-магазины, интернет-сайты.

Кейс № 2

1 СИТУАЦИЯ

Вам нужно снять деньги с карты. На противоположной стороне улицы в стену магазина встроен уличный банкомат. Улица плохо освещена и возле банкомата стоят какие-то люди. Ваши действия?

ЭКСПЕРТ

Старайтесь пользоваться банкоматами внутри отделений банков. Их чаще проверяют и лучше охраняют.

Проверьте банкомат: нет ли на нем посторонних устройств. Клавиатура не должна отличаться по фактуре, а тем более шататься.

Когда вводите ПИН-код, всегда прикрывайте клавиатуру свободной рукой, чтобы никто не подсмотрел.

Лучше всего, если на банкомате есть «крылья» для клавиатуры — на них невозможно поставить накладную клавиатуру. Также благодаря им сложнее подсмотреть ваш ПИН-код.

---

2 СИТУАЦИЯ

Вы снимаете деньги в офисе банка, довольно близко от вас стоит молодой человек и, дружелюбно улыбаясь, наблюдает за тем, как вы вводите ПИН-код на клавиатуре банкомата. Ваши действия?

ЭКСПЕРТ

Не стоит ссориться, но нужно прикрыть клавиатуру рукой в тот момент, когда вы будете набирать ПИН-код, и постараться закрыть собой монитор банкомата, чтобы никто не видел, какие именно операции вы совершаете по карте.

---

3 СИТУАЦИЯ

Вам на мобильный телефон звонит человек и, представляясь сотрудником банка, сообщает, что по вашей банковской карте была проведена подозрительная операция, из-за чего банк заблокировал карту. Для разблокировки вам необходимо сейчас сообщить всю важную информацию: ФИО, номер карты, ПИН-код, трехзначный код на оборотной стороне карты. Ваши действия?

ЭКСПЕРТ

Сотрудники банка владеют необходимой информацией для блокировки карты. Им незачем спрашивать ее у вас. Не реагируйте на подобный звонок, в случае сомнений перезвоните в банк по телефону, указанному на оборотной стороне карты.

---

4 СИТУАЦИЯ

На мобильный телефон вам пришло сообщение: «Поздравляем, вы стали тысячным посетителем нашего сайта. Вы выиграли ноутбук! Это не розыгрыш, перешлите на указанный номер x-xxx-xxx-xx-xx фото своего паспорта, номер телефона, мы вам перезвоним для отправки ноутбука». Ваши действия?

ЭКСПЕРТ

Таким образом мошенники пытаются выудить у вас персональные данные (паспорта, банковской карты). Как говорится, бесплатный сыр бывает только в мышеловке. Не верьте подобной информации, не отправляйте свои данные мошенникам.

Кейс № 3

1 СИТУАЦИЯ

На вашу электронную почту приходит письмо с адреса известной платежной системы: «Мы подвели итоги лотереи держателей карт нашей платежной системы. Поздравляем вас с победой в конкурсе! Перейдите по ссылке для получения приза». Вы перешли по ссылке и видите знакомую вам страницу сайта, правда, немного худшего качества, чем всегда (логотип платежной системы какой-то нечеткий). Перед вами форма для заполнения информации по вашей карте, куда вам перечислят деньги. Ваши действия?

ЭКСПЕРТ

Мошенники копируют известные сайты, используя похожее название компании и оформление. Например, вы хотите узнать, поступила ли стипендия на вашу карту, вводите логин и пароль на сайте банка, а попадаете на сайт-клон. Если вы введете на таких сайтах свои данные, они попадут в руки злоумышленников. В данном случае о том, что это сайт-клон, говорит нечеткое изображение логотипа. Если попробуете открыть другие страницы сайта, они могут не открываться.

---

2 СИТУАЦИЯ

На мобильный телефон / электронную почту вам пришло сообщение: «Добрый день, будущий коллега! Хочу предложить тебе интересную, высокооплачиваемую работу. Я вижу, ты очень активен в социальных сетях, поэтому предлагаю тебе размещать посты о нашей компании

в интернете. Работенка непыльная, оплата 1000 долларов США в месяц. Торопись, друг, подобное письмо я направил еще нескольким парням, кто первый из вас перейдет по ссылке _____, тот и получит работу своей мечты!». Ваши действия?

ЭКСПЕРТ

Перейдя по такой ссылке, вы не найдете работу мечты — разве что компьютерный вирус. Будьте осторожны, получая предложения легкого заработка.

---

3 СИТУАЦИЯ

На ваш мобильный телефон пришло сообщение: «Вам поступил платеж 200 рублей». При этом вы не пополняли счет своего телефона. Вы удивлены. Через 10-15 минут приходит новое сообщение: «Извините, ошибочно перевела 200 рублей на ваш счет. Пожалуйста, верните деньги на мой номер х-ххх-ххх-хх-хх. Лиза». Ваши действия?

ЭКСПЕРТ

Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не поступали, СМС пришло не от вашего оператора, а повторное СМС прислал вам злоумышленник. Проверьте состояние вашего счета, закажите выписку у оператора или позвоните службу поддержки, прежде чем переводить кому-то деньги.

---

4 СИТУАЦИЯ

Вы зашли на страницу банка, картой которого Вы пользуетесь, для того, чтобы оплатить мобильную связь. Вас немного насторожило, что страница сайта выглядит как-то иначе, в названии банка допущена ошибка, ссылки, по которым вы собираетесь пройти, не работают. Но возможность совершить оплату присутствует. Ваши действия?

ЭКСПЕРТ

Возможно, ваш смартфон заражен вирусом, который перенаправил вас с официального сайта банка на сайт-клон, похожий как две капли воды на оригинальный сайт. Если вы введете информацию по карте, то ваши деньги уйдут мошенникам. Чтобы обезопасить себя, набирайте вручную адрес сайта, не переходите по ссылкам из интернета. Делайте покупки только на сайтах, которые обеспечивают безопасное соединение. Адрес такого ресурса начинается с https://. В адресной строке есть значок в виде закрытого замка.
