

# ПАМЯТКА

## «Алгоритмы действий интернет-мошенников в сети Интернет: как не стать жертвой киберпреступника»

### ФИШИНГ (вредоносные ссылки на поддельные Интернет-ресурсы):

- Вы выкладываете объявление о продаже товара на торговых площадках («Kufar», «Из рук в руки» и др.);
- С вами связывается «Потенциальный покупатель» посредством различных мессенджеров (Viber, WhatsApp, Telegram);
- Неизвестный интересуется товаром, а после предлагает приобрести товар, используя «Куфар-доставку» или «Европочту», «СДЕК-доставку»;
- Предоставляет ссылку, внешне схожую с официальной «Куфар-доставка», «Европочта» или «СДЕК-доставка», в которой необходимо якобы для получения оплаты за товар вести личные данные, а именно: паспортные данные, реквизиты банковской платёжной карты и код подтверждения операции, полученный в сообщении от банка;
- Так как данная ссылка, не официальная, а созданная человеком, который ее отправил, **ВСЕ** Ваши личные данные отправляются ему. С использованием полученных данных интернет-мошенники могут оформить на Вас кредит и перевести денежные средства, находящиеся на Ваших банковских картах на свои счета.

Аналогичным способом совершаются и другие преступления, связанные с переходом на сторонние Интернет-ресурсы, где необходимо ввести личные данные, также логины и пароли от аккаунтов (Steam, социальные сети и иные программные продукты).

**Вывод: если вы недостаточно уверены в подлинности ссылок, которые Вы открываете, а также куда вводите свои личные данные, не в коем случае нельзя по ним переходить.**

### ВИШИНГ (неизвестные лица представляются сотрудниками милиции или банка):

- Посредством различных мессенджеров (Viber, WhatsApp, Telegram) или по средствам обычной связи как от иностранных номеров, так и от Белорусских поступают звонки;
- Собеседник представляется сотрудником милиции или банка;
- В ходе диалога сообщает, что:

На Ваше имя оформлен кредит	Вы стали жертвой преступления	Ваши родные и близкие попали в беду (Мошенник просит перевести деньги на его счет для благополучного решения вопроса)
-----------------------------	-------------------------------	--

Как правило в большинстве случаев неизвестные пытаются узнать ваши личные данные, а также просят установить приложение «AnyDesk» или «TeamViver», которые якобы обезопасят Ваши данные. Данные приложения на самом деле предназначены для удаленного доступа к Вашему телефону. Установив их, мошенник получает полный доступ к Вашему устройству и может совершать любые действия на нем, в иных случаях просто просят предоставить СМС-сообщения с кодами, полученные от банка (либо просит войти в СМС-сообщения). Данные коды предназначены для прохождения авторизации в Вашем мобильном банкинге или совершения расходных операций в Интернете.

**Вывод: не скачивать сторонние программы пока вы не убедились в точном его функциональном предназначении. Не предоставлять личные данные, а также коды для проведения операций, полученные в сообщении от банков. Сразу связываться с настоящими сотрудниками банков по абонентским номерам, указанным на оборотной стороне Вашей банковской карты или официальном сайте. При получении информации о беде, случившейся с родственниками, сразу связывайтесь с ними и уточняйте о действительности данных обстоятельств, ни в коем случае не переводить денежные средства по просьбе неизвестных лиц на иные счета.**

### Иные преступления:

К иным преступлениям, совершаемым в сети интернет можно отнести: мошенническое завладение денежными средствами в социальных сетях и мессенджерах:

- Вы хотите приобрести товар, объявление о продаже которого размещено пользователем социальной сети (Instagram, ВКонтакте, Telegram и иных), в каком-либо сообществе или на «стене» пользователя;
- Продавец предлагает Вам внести полный платеж либо предоплату до получения товара;
- Вы переводите денежные средства на предоставленный счет (карту), однако приобретаемый товар вы не получили, а после перевода денег на связь продавец не выходит.

**Вывод: необходимо перед переводом денег ознакомиться с отзывами о продавце, а также не вносить полный платеж за товар до его получения, удостовериться в действительности продавца и наличии товара.**

## **СПРАВКА ОБ ОЗНАКОМЛЕНИИ**

С памяткой на тему: «Алгоритмы действий интернет-мошенников в сети Интернет: как не стать жертвой киберпреступника» ознакомился путем личного прочтения, копию памятки получил.

---

---

---

---

---

(ФИО; число, месяц, год рождения; адрес места жительства; мобильный телефон)

\_\_\_\_\_  
(дата ознакомления)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(инициалы, фамилия)

ОЗНАКОМИЛ И КОПИЮ ПАМЯТКИ ВЫДАЛ:

---

---

---

---

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(инициалы, фамилия)

## **СПРАВКА ОБ ОЗНАКОМЛЕНИИ**

С памяткой на тему: «Алгоритмы действий интернет-мошенников в сети Интернет: как не стать жертвой киберпреступника» ознакомился путем личного прочтения, копию памятки получил.

---

---

---

---

---

(ФИО; число, месяц, год рождения; адрес места жительства; мобильный телефон)

\_\_\_\_\_  
(дата ознакомления)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(инициалы, фамилия)

ОЗНАКОМИЛ И КОПИЮ ПАМЯТКИ ВЫДАЛ:

---

---

---

---

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(инициалы, фамилия)