



Дистанционное мошенничество в отношении несовершеннолетних

**Кашкарова Наталья
Алексеевна**

начальник отдела информации и
общественных связей МВД по Республике
Крым, полковник внутренней службы





Дистанционное мошенничество



**злоумышленник, используя
компьютерные и
телефонные сети, путем
обмана, склоняет к
передаче денег**

Дистанционное мошенничество в отношении несовершеннолетних

1

«ФИШИНГ»

2

Фальшивые интернет-магазины

3

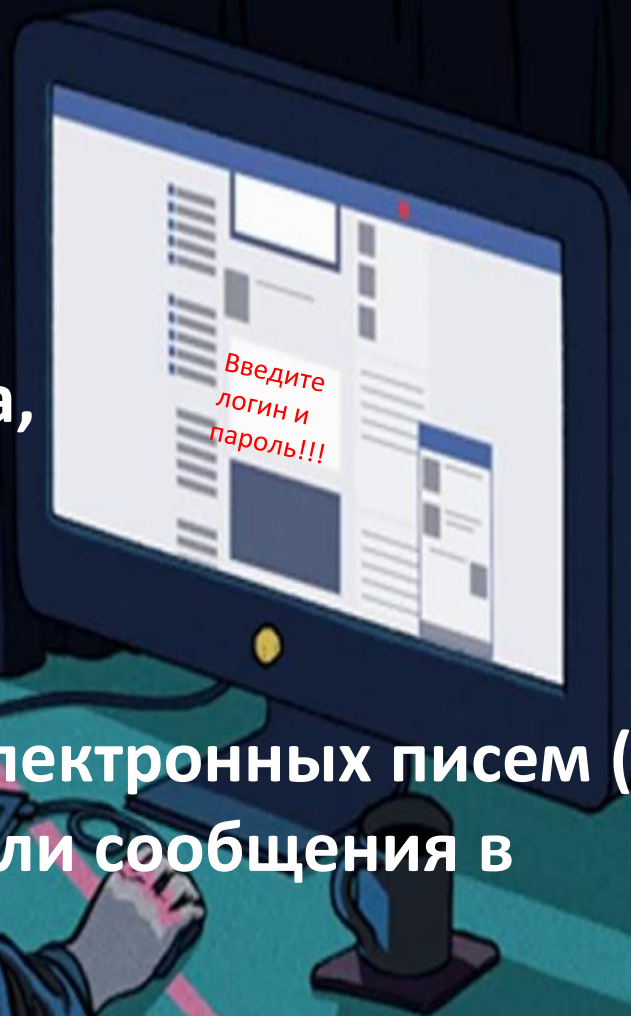
Взлом личной страницы в социальной сети с целью просьб о помощи

ФИШИНГ

✓ вид интернет-мошенничества, при котором получается доступ к логинам и паролям.

✓ достигается путём рассылки электронных писем (от имени популярных брендов или сообщения в социальных сетях).

✓ в сообщении содержится ссылка на сайт, внешне неотличимый от настоящего, где нужно авторизоваться (ввести логин и пароль от личной



<http://vkontakte.ru/>

В контакте

E-mail или Логин

Пароль:

Войти

Забыли пароль?

Добро пожаловать

ВКонтакте – универсальный сервис, которым ежедневно пользуются миллионы людей.

С помощью **ВКонтакте** вы можете:

- Найти людей, которых вы давно не видели
- Узнать больше о своих друзьях

госуслуги



Госпочта – для важных писем

Получайте уведомления и заказывайте от госслужбы не вбукашки с электронной почты.

Получить

Популярные на портале

Получить записку

Узнать результаты ЕГЭ

Правила сайта

Заняться спортом

Открыть свой бизнес

gosuslugis.ru



Nordea

Netbank

Beliggenhed verifikation

Beliggenhed kontoplysning

Kreditkortnummer

Udløbsdatoen

Sikkerhedskode

CPR-nr

Fortsæt

Осторожно, фишинг!
Введение данных на этой странице может привести к их краже.

OK

[Ændre bruger-id og log på](#)

[Ændre adgangskode og log på](#)

Denne forbindelse er sikret af SSL-kryptering. For at kontrollere at du har forbindelse til Nordea, kan du klikke på hængelåsen.



В <http://vka.com>

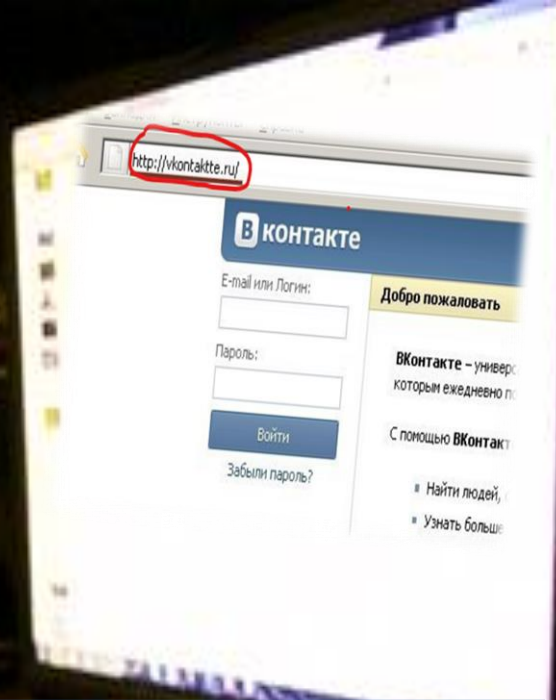
В контакте

Телефон или email

Пароль



РЕКОМЕНДАЦИИ



- ✓ не переходите по ссылкам, которые присылают Вам незнакомые люди
- ✓ не переходите по ссылкам на сайты, которые Вам не знакомы
- ✓ не вводите для входа на незнакомые сайты логин/пароль от Ваших соцсетей!

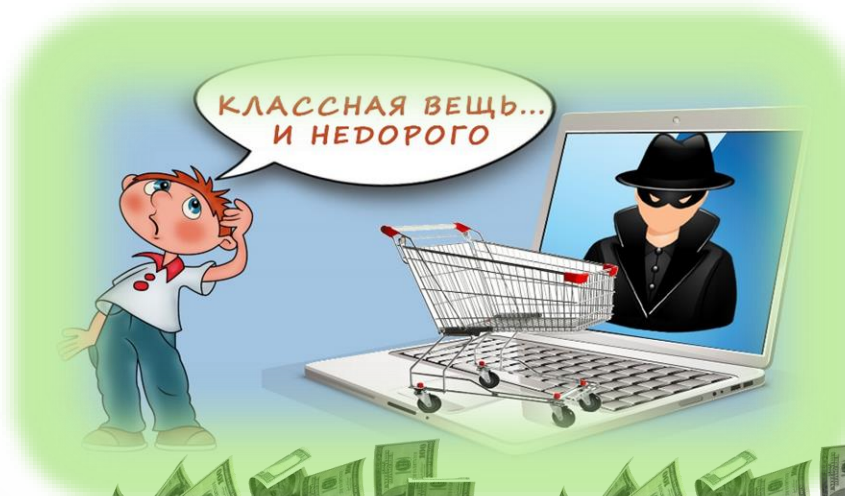
ФАЛЬШИВЫЕ ИНТЕРНЕТ-МАГАЗИНЫ

- ✓ злоумышленник размещает товар, получает оплату за него (либо часть оплаты) и далее не выходит на связь.
- ✓ это могут быть как и сайты в интернете, так и профили магазинов в соцсетях!



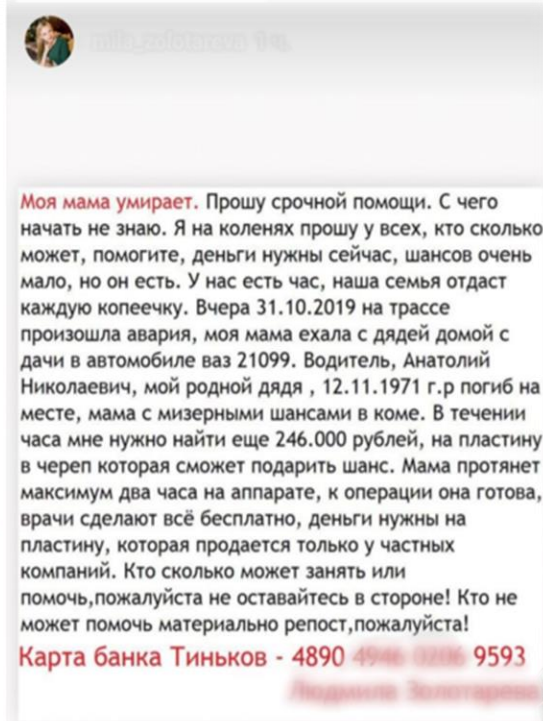
НА ЧТО ОБРАТИТЬ ВНИМАНИЕ?

- ✓ дата создания сайта (Если создан недавно, должны возникнуть подозрения)
- ✓ упоминания в сети (Всю информацию можно узнать в интернете, введя название в поисковик)
- ✓ отзывы (Их могут накрутить. Стоит посмотреть, от кого оставлены отзывы, с каким промежутком времени)
- ✓ подозрительно низкая цена товара! (Для привлечения внимания)



Взлом личной страницы в социальной сети с целью просьб о помощи

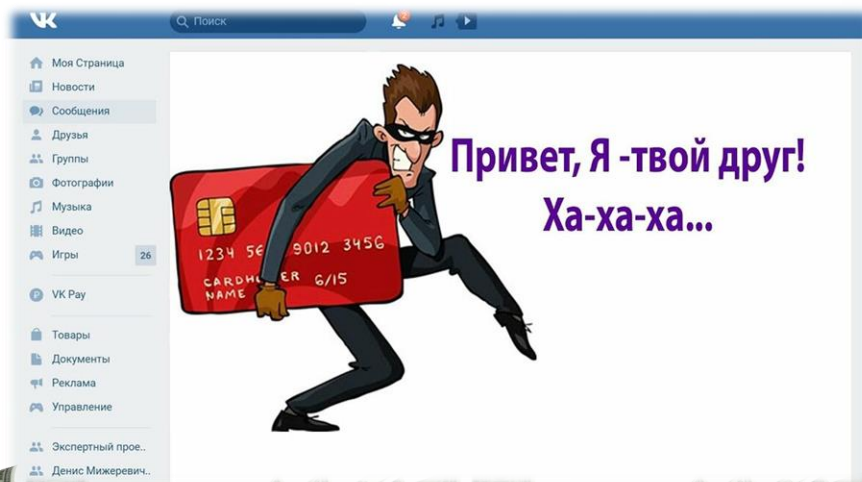
✓ мошенники взламывают персональную страницу пользователя в социальных сетях и отправляют сообщения с просьбой помочь (срочно перевести деньги)



РЕКОМЕНДАЦИЯ:

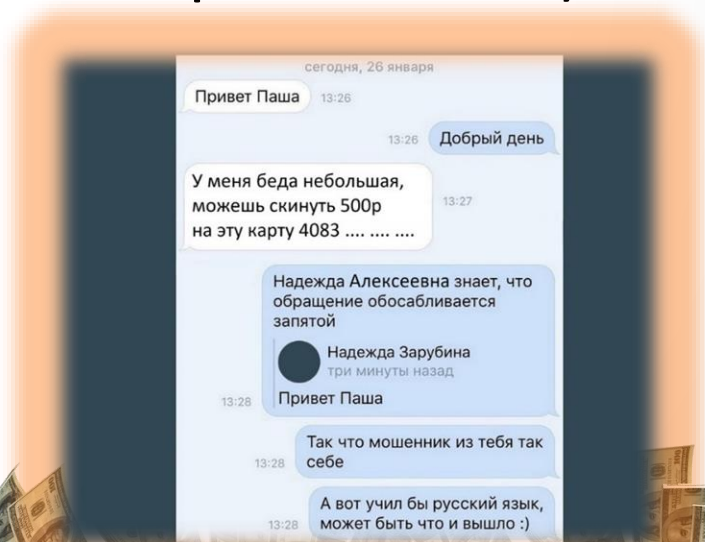
✓ позаботитесь о пароле для своего аккаунта в соцсетях. Он защищает не только вашу безопасность, но и безопасность ваших родных и близких

- 1) если записываете – храните в недоступном для других месте;
- 2) используйте разные пароли для разных соцсетей;
- 3) никому не называйте свои пароли;
- 4) не вводите логин и пароль на сайтах, на которые Вы перешли по ссылке!



Что делать, если вам пришло сообщение с просьбой о помощи от одного из знакомых или родственников?

- ✓ необходимо немедленно связаться с ним по телефону, уточнить отправлял ли он это сообщение и не предпринимать ничего, пока он не подтвердит это лично;
- ✓ нельзя сообщать реквизиты карты (три цифры на оборотной стороне, срок действия, пароль из смс)



За этот год в Крыму произошло 6 дистанционных мошенничеств в отношении несовершеннолетних

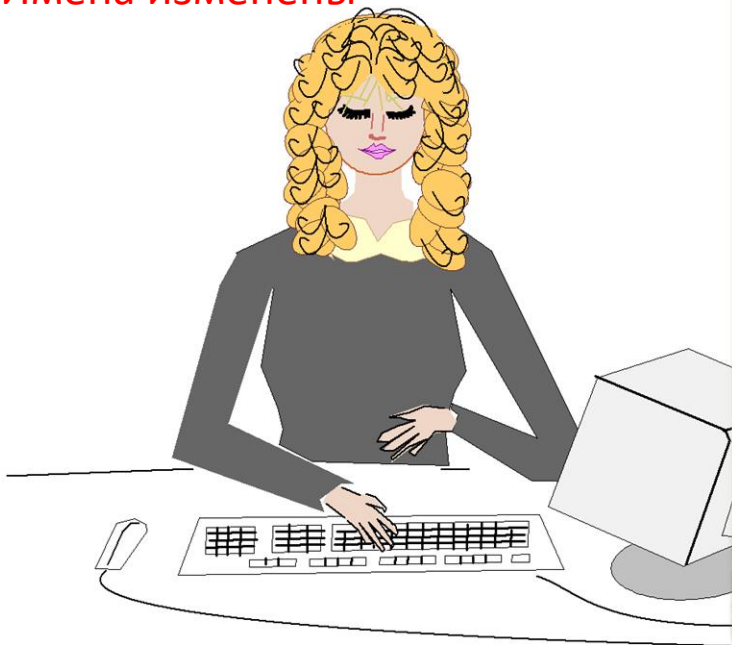
- ✓ потерпевшие обратились в правоохранительные органы
- ✓ сотрудники полиции помогают восстановить справедливость



Случаи, произошедшие в Крыму

✓ 6 августа в Красногвардейском р-не, злоумышленник воспользовался чужой страницей соцсети «ВКонтакте», представился Кате* её знакомой Аллой* и попросил займы 3000 рублей. Катя* не знала, что со страницы её знакомой пишет совсем другой человек и перечислила деньги.

*Имена изменены



Когда Катя* поняла, что её обманули, она обратилась в полицию, чтобы ей помогли.



✓ 28 февраля злоумышленник разместил неправдивую информацию в соцсети «Instagram» и «Telegram» и путём обмана получил деньги 17-летнего Сергея*. Мальчик перечислил злодею 15 200 рублей.



Сергей обратился в полицию. Полицейские возбудили уголовное дело и привлекут злоумышленника к ответственности.



- ✓ В августе 15-летний Богдан* из Керчи хотел купить себе мопед, собирал деньги.
- ✓ Гуляя в одной компании, 21-летний Тимофей* слышал об этом. Он решил обмануть Богдана*, написал ему «Вконтакте» и предложил купить мопед за 5 000 рублей. При этом, мопеда у него никогда не было.
- ✓ Богдан* согласился и передал ему деньги.
- ✓ Тимофей* не выходил на связь и скрылся.



Богдан* с мамой обратились в полицию, сотрудники полиции нашли Тимофея* и привлекут его к ответственности.



Далее рассмотрим ситуации

- прочитайте историю и подумайте, как бы Вы поступили



СИТУАЦИЯ 1.

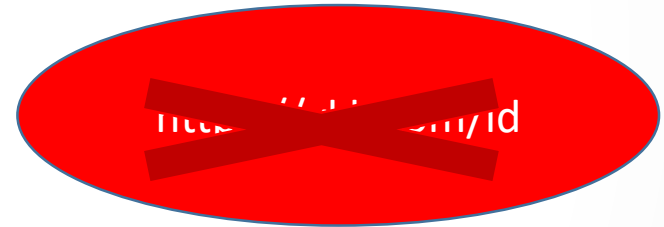
- твоя подруга Аня прислала ссылку в соцсети «Вконтакте» с просьбой проголосовать за её сестру в конкурсе.
- перейдя по ссылке, нужно ещё раз войти на личную страницу «Вконтакте» и заново ввести логин и пароль.

КАК ВЫ ПОСТУПИТЕ?



ОТВЕТ:

- 1) если есть возможность, лично уточнить у подруги Ани, присылала ли она сообщение с просьбой проголосовать.
- 2) не вводить заново логин и пароль, вход на настоящую страничку уже был.
- 3) проверить, похожа ли ссылка на настоящую:



СИТУАЦИЯ 2.

- Максим Давно хотел себе гироскутер, но ему не хватало на него денег.
- В интернете он находит сайт с очень низкими ценами, потому что интернет-магазин только появился.
- Максим посмотрел, что уже много людей купили гироскутеры и оставили хорошие отзывы.

Что еще нужно сделать Максиму?



ОТВЕТ:

- 1) почитать отзывы о сайте в интернете. Если отзывы плохие или их совсем нет – это могут быть мошенники.
- 2) помнить о том, что очень низкие цены могут быть для привлечения внимания. Лучше посоветоваться об этом со старшими.
- 3) посмотреть, от реальных ли людей оставлены отзывы на товар или от вымышленных страниц.



СИТУАЦИЯ 3.

- Оля откладывала деньги, чтобы потом себе что-нибудь купить.
- В соцсети ей пришло сообщение от друга Димы о том, что ему нужна помощь. Очень срочно нужно отправить ему деньги, которые он вернёт уже вечером.
- Оле не жалко, ведь деньги пока что ей не нужны, а Дима её хороший друг и быстро их вернёт.

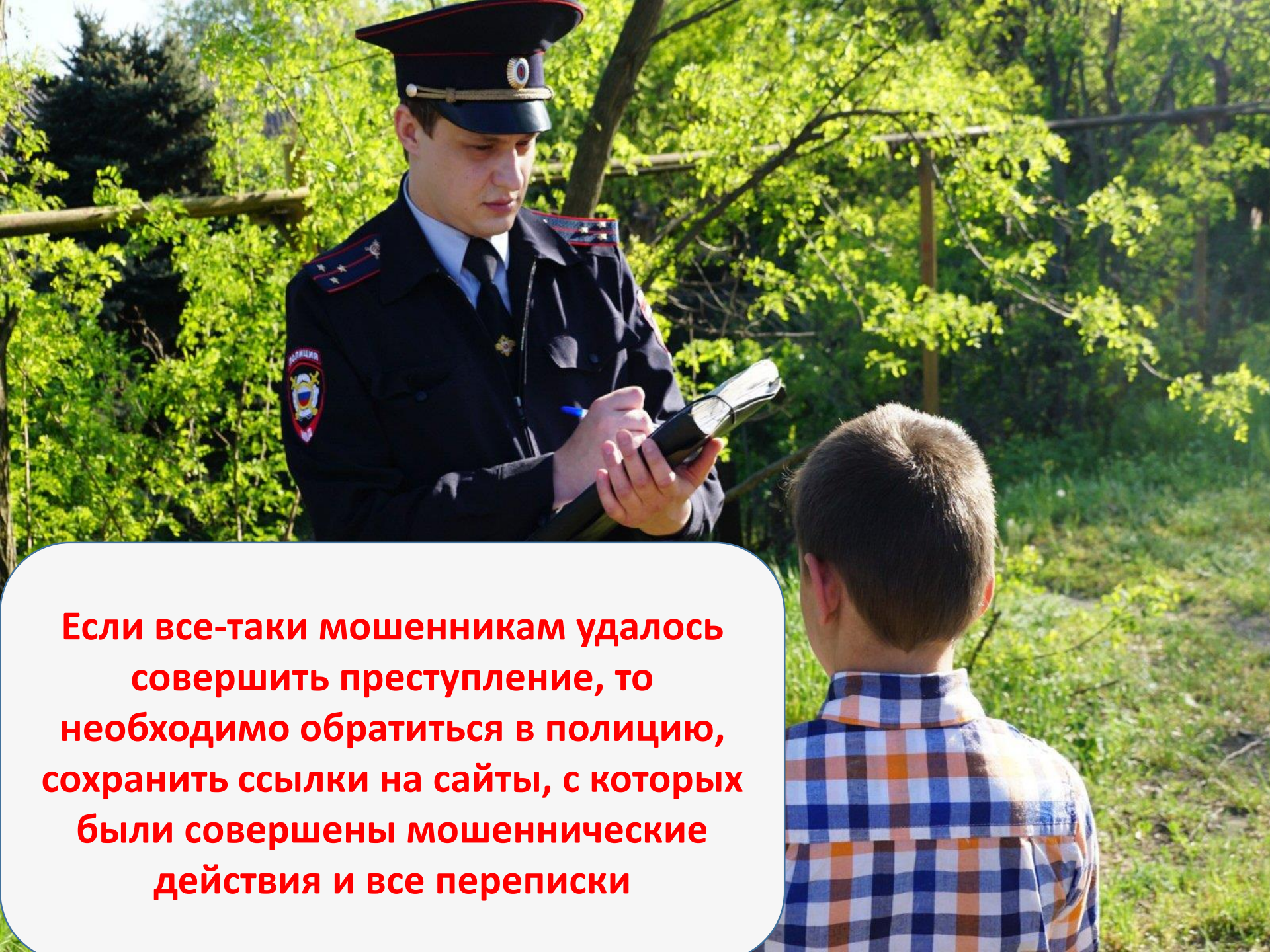
Как Оле себя обезопасить?



Ответ:

- 1) Позвонить или лично встретиться с другом Димой, которому она хочет переслать деньги.
- 2) если она убедилась в том, что страница друга взломана другим человеком, быстро об этом рассказать Диме, чтобы он поменял пароль!
- 3) распространить информацию о том, что страница друга взломана!





Если все-таки мошенникам удалось совершить преступление, то необходимо обратиться в полицию, сохранить ссылки на сайты, с которых были совершены мошеннические действия и все переписки