УВД ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА
КРИМИНАЛЬНАЯ МИЛИЦИЯ
УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

# ОПОРНЫЙ ПЛАН-КОНСПЕКТ

Тема:
«Что такое фишинг? Как защитить себя от фишинга»

Гомель
2022 год

За последние десятилетия число киберпреступлений в мире увеличилось в огромное количество раз, мотивы и цели киберпреступников менялись с течением времени, а опасность совершаемых преступлений возрастает с каждым годом. Этому свидетельствуют огромные финансовые потери юридических лиц и структур, а также участившиеся случаи киберпреступлений и против физических лиц.

В Гомельской области с 2017 года наблюдался устойчивый рост таких преступлений (2017 г. – 370, 2018 г. – 563, 2019 г. – 1781, 2020 г. – 3394). В 2022 году количество преступлений снизилось, за 2 месяцев текущего года в Гомельской области зарегистрировано 295 киберпреступлений, что в 1,9 раза меньше данного показателя 2021 года (561 преступление). Более 90% из выявленных преступлений составляют хищения имущества путем модификации компьютерной информации (ст. 212 УК Республики Беларусь). Кроме этого, отмечается рост количества преступлений в сфере информационной безопасности (28).

В дальнейшем прогнозируется, что развитие IT-отрасли и финансово-кредитной сферы, будут способствовать сохранению тенденции совершения преступлений по направлению противодействия киберпреступности.

В национальном сегменте сети Интернет Республики Беларусь наблюдается значительное повышение мошеннической активности, связанной с использованием **фишинговых страниц** и даже целых сайтов.

Целью данной разновидности фишинга является получение не только учетных данных от каких-либо сервисов (логин и пароль), но и данных платежной карты (номер, срок действия, имя и фамилия держателя и CVC2/CVV2 код).

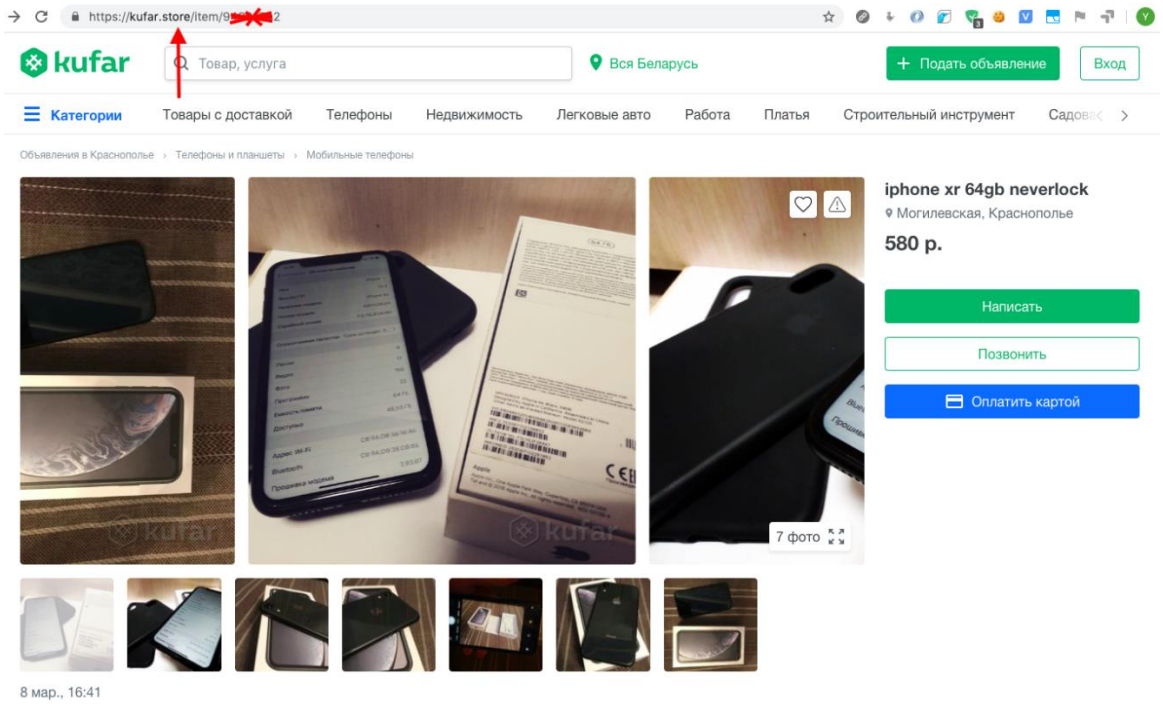
Также стоит отметить, что продуманный целевой фишинг не обходится без использования социальной инженерии. Причем если раньше в основном происходила рассылка фишинговых писем на электронную почту, где была возможность блокировать массовые рассылки, то теперь злоумышленники используют еще мессенджеры и социальные сети, что значительно расширяет целевую аудиторию.

**Что такое фишинг? Как защитить себя от фишинга?**
(по информации предоставленной службой поддержки пользователей «Куфар»)

**Фишинг** - это вид мошенничества в интернете, направленный на то, чтобы получить личные данные пользователей (логины, пароли, номера карт, смс-коды от банков и т.д.), а затем использовать их для кражи денег с карты или совершения других недобросовестных действий.

**В чём заключается фишинг?**

Мошенники создают страницу, которая визуально очень похожа на страницу реально существующей компании или вовсе идентична ей. Размещают её на сайте, название которого визуально тоже очень похоже на название реальной компании и имеет лишь незначительные различия. Отправив такую ссылку пользователю, они ждут, когда он введёт на такой странице свои данные. Как только он это сделает, данные окажутся в руках мошенников, и они смогут их использовать по своему усмотрению. Вот, например, как выглядит фишинговая страница, которая маскируется под Куфар. Обратите внимание, внешний вид абсолютно идентичен Куфару, **выдаёт обман только адрес страницы (вместо .by указано .store):**



**Под каким предлогом мошенники могут выслать вам ссылку на фишинговую страницу?**

Вот актуальные схемы, которыми мошенники завлекают людей:

**1. Фишинговая страница, которая выглядит как интернет-банк.** Мошенник под видом покупателя пишет продавцу о желании приобрести товар, а также сообщает, что прямо сейчас забрать его не может. Чтобы продавец гарантированно его оставил, предлагает перевести деньги продавцу немедленно, а для этого спрашивает, какой у него банк и номер карты. После чего сообщает, что нужно подтвердить перевод, высылает ссылку на поддельную страницу, выглядящую как интернет-банк, где пользователю предлагается ввести свои данные для входа в интернет-банк, а затем ввести код из смс. Если пользователь введёт свои данные, то мошенник сможет от его имени зайти в интернет-банк и перевести деньги куда угодно.

**2. Фишинговая страница, которая выглядит как Куфар.** Мошенник размещает объявление о дорогостоящем товаре по привлекательной цене. Пишет в объявлении, что связь только через мессенджер (Viber, WhatsApp, Telegram), после чего получает телефоны заинтересованных пользователей в личные сообщения. Пишет им в месенджере, что готов продать товар, но так как находится в другом городе, то вышлет вещь через Куфар Доставку. После чего высылает ссылку на страницу, которая выглядит совершенно так же, как Куфар, и на которой предлагается ввести свои данные карты для оплаты за товар. Если доверчивый пользователь вводит свои данные, то мошенник с их помощью переводит деньги с карты пользователя на свой счёт.

**Как узнать, что страница настоящая?**

• **Адресная строка.** Поищите официальный сайт компании в Гугле или Яндексе и сравните написание этого сайта с тем, которое вы видите на странице, которую вам кто-то выслал. Например, **kufar.by** -- это реальное название. А kufar.be, kufar.store, kufar.swf.com, kufar.aa.by нашими названиями не являются.

**Настоящими ссылками на Куфар являются только ссылки, которые начинаются так:**

www.kufar.by (Куфар),
https://auto.kufar.by/ (Куфар Авто),
https://re.kufar.by/ (Куфар Недвижимость),

https://rassrochka.kufar.by/ (Куфар Рассрочка),
https://kufar.by/rassrochka(Переводы в рассрочку),
https://perevod.kufar.by/ (Страница P2P-переводов),
https://business.kufar.by/ (Куфар Бизнес),
https://support.kufar.by/hc/ru (Служба поддержки пользователей).

• **Другие элементы страницы.** Они могут выглядеть как настоящие, но на самом деле такими не являются. Например, при нажатии на кнопку ничего не происходит; в меню ни один пункт никуда не ведёт.

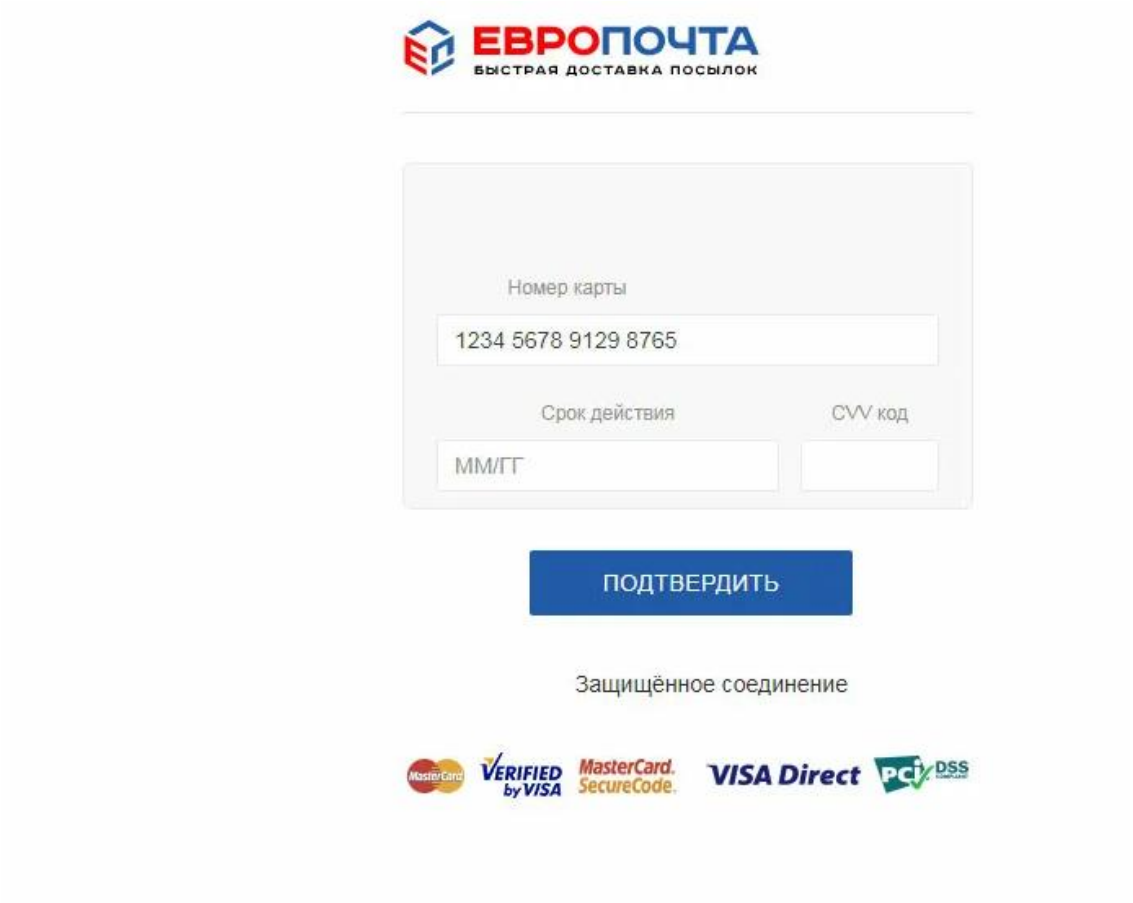
• **Особенности текста.** Даже одна-единственная странность может указывать на то, что страница не настоящая. Например, написание "Белорус Банк" вместо "Беларусбанк".

**Как ещё можно себя обезопасить?**

• **Вести переписку только на Куфаре**. На официальном сайте Куфара заблокирована возможность отправлять ссылки на сторонние сайты, и это сделано специально для того, чтобы оградить граждан от попыток недобросовестных пользователей увести на мошенническую страницу. Если кто-то хочет отправить вам ссылку на объявление на Куфаре, то в личных сообщениях это можно сделать. Однако если это фишинговая страница (т.е. выглядит как Куфар, но на самом деле Куфаром не является), то отправить ссылку на неё в личных сообщениях не получится.

• Если нужно перевести деньги на другую карту, то необходимо пользоваться мобильным приложением от вашего банка, либо же самостоятельно заходить на страницу интернет-банка вашего банка, сохраните себе её в закладки. Не переходите по ссылкам, которые вам высылают посторонние люди.

Также продолжают регистрироваться случаи мошенничества среди сайтов-подделок почтового оператора «Европочта». **Официальный сайт «Европочты» – https://evropochta.by/.** Все другие адреса сайтов являются поддельными и не имеют никакого отношения к почтовому оператору! По информации официального сайта «Европочта» вот лишь некоторые адреса поддельных сайтов мошенников (ewropost.by, evropochta.club, evropochta.me, evropost.site, evropochta.co, evropochta.cc, evroposhta.by).




На этих сайтах мошенники под видом «Европочты» требовали ввести реквизиты банковской платежной карты для оплаты и тем самым похищали денежные средства граждан. На данный момент компанией приняты все необходимые меры для блокировки мошеннических сайтов

**Будьте бдительны! Европочта информирует, что она никогда не запрашивает данные по банковским платежным картам клиентов.** Все оплаты происходят в отделениях почтовой связи.