Следчы камітэт
Рэспублікі Беларусь

Следственный комитет
Республики Беларусь

Упраўленне па
Гомельскай вобласці

Управление по
Гомельской области

246050, г. Гомель,
вул. Савецкая, 34
тэл. 8 (0232) 69 30 04,
факс 8 (0232) 69 31 58
e-mail: GM@sk.gov.by

246050, г. Гомель,
ул. Советская, 34
тел. 8 (0232) 69 30 04,
факс 8 (0232) 69 31 58
e-mail: GM@sk.gov.by

13.04.2021 № 18-2/6427

на № _____ ад _____

Председателю
Гомельского областного
исполнительного комитета
Соловью Г.М.

О профилактических мерах по предупреждению преступлений

Уважаемый Геннадий Михайлович!

Управлением Следственного комитета Республики Беларусь по Гомельской области (далее – УСК) постоянно уделяется внимание вопросам профилактической работы по предупреждению преступлений в сфере высоких технологий, в особенности, возбужденных по ст. 212 Уголовного кодекса (хищение путём использования компьютерной техники).

Несмотря на принимаемые УСК и другими субъектами профилактики меры статистические сведения о состоянии преступности в Республике Беларусь свидетельствуют об устойчивой динамике роста количества совершаемых преступлений в сфере высоких технологий.

Характерным является то, что число зарегистрированных в 2020 году в республике преступлений в сфере высоких технологий (25575) более чем в 12 раз превысило общее количество совершенных за тот же период убийств (306), причинения тяжких и менее тяжких телесных повреждений (755 и 533 соответственно), изнасилований (64), насильственных действий сексуального характера (268) и разбоев (81) вместе взятых.

За 2020 год мошенники похитили у банковских клиентов с их карт и счетов свыше 1 580 000 рублей (только по раскрытым и направленным в суд уголовным делам), совершив более 23 000 несанкционированных операций.

В области, как и в республике в целом, отмечается рост количества совершаемых преступлений в сфере высоких технологий.

Если за 3 месяца 2020 года на территории Гомельской области зарегистрировано 246 преступлений по ст. 212 Уголовного кодекса, то за аналогичный период этого года количество таких преступлений увеличилось более чем в три раза – 751.

Приведённая статистика свидетельствуют о недостаточной осведомлённости отдельных граждан о подобных фактах, что требует активизации работы по предупреждению данных преступлений всеми

субъектами профилактики, усилия которых, по нашему мнению, в первую очередь, должны быть направлены на информирование населения о возможных рисках и последствиях передачи своих персональных данных третьим лицам.

Сотрудники УСК ежемесячно выступают в средствах массовой информации, трудовых коллективах с разъяснениями о способах совершения хищений денежных средств граждан посредством интернет-мошенничества, рассказывают о финансовой грамотности и мерах предосторожности при пользовании банковскими карточками.

К примеру, 26.03.2021 на телеканале «Мозырь» вышел сюжет о встрече начальника УСК с коллективом ОАО «Мозырьсоль», в котором была обозначена проблема роста в регионе киберпреступлений.

05.04.2021 на телеканале «Нюанс» в программе «Жлобин-Инфо» вышло расширенное интервью начальника Жлобинского РОСК о преступлениях в сфере высоких технологий и их профилактики.

Для качественного расследования данных преступлений организуются обучающие мероприятия по подготовке сотрудников, специализирующихся на расследовании преступлений против информационной безопасности. Практикуется проведение с другими правоохранительными органами рабочих встреч и координационных совещаний.

В текущем году увеличен штат сотрудников специализированного отдела следственного управления УСК, который непосредственно занимается расследованием данного вида преступлений.

В целях предупреждения совершения преступлений в сфере высоких технологий, снижения количества жертв интернет-мошенников в следственные подразделения области направлено указание начальника УСК от 09.04.2021 «О профилактике преступлений в сфере высоких технологий», в котором руководителям территориальных отделов предписано направить в местные исполнительные и распорядительные органы для размещения на информационных стендах и иных специально отведенных местах, на сайтах районных, городских газет, сайтах райисполкомов, горисполкома профилактические материалы, разработанные центральным аппаратом Следственного комитета совместно с Белорусским телеграфным агентством.

По-прежнему является актуальным использование аудио-визуального информирования граждан в общественном транспорте и в учреждениях торговли, размещение соответствующей информации на бумажных листовках в подъездах жилых домов, лифтах, а также её размещение на счетах оплаты за коммунальные услуги.

Ранее в Гомельский областной исполнительный комитет также направлялись письма с предложениями о принятии дополнительных мер по предупреждению данного вида преступлений (от 05.12.2019 №18-3/19108, от 29.12.2020 №18-1/6504).

Кроме того, полагаем возможным инициирование Гомельским областным исполнительным комитетом внесение местными органами власти предписаний в учреждения, предприятия и организации области о необходимости надлежащего доведения профилактической информации до каждого сотрудника и работника.

Полагаем, что реализация указанных мероприятий позволит снизить количество пострадавших от данного вида преступлений.

Приложение: информационные материалы на 6 л.

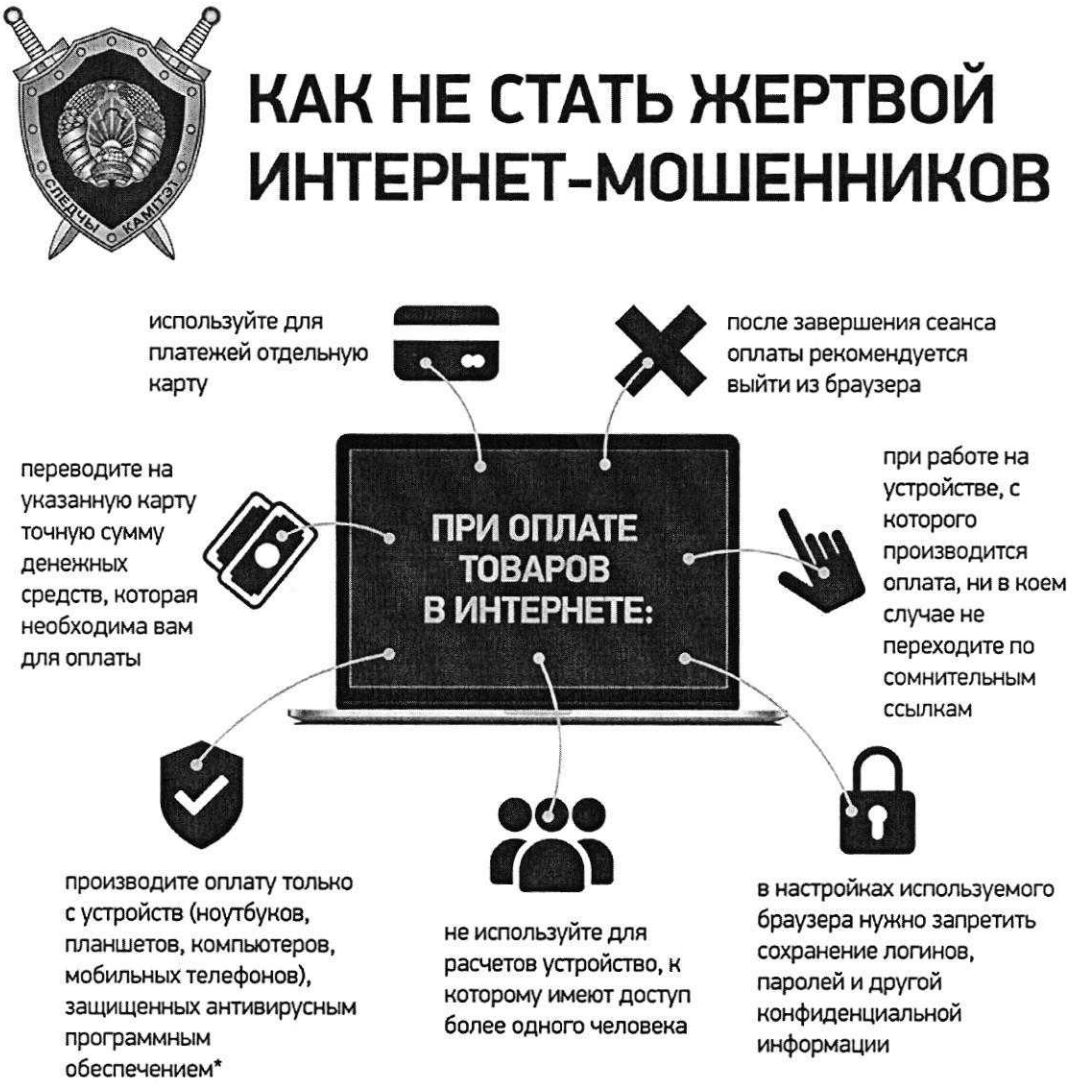
С уважением,

Начальник управления С.А.Удовиков

2 Мельгуй С.А. (80232) 69-30-08

ИНФОГРАФИКА
09 АПРЕЛЯ 2021, 14:17

Как не стать жертвой интернет-мошенников



**Антивирус должен быть включен, антивирусные базы и программа - обновляться, следует регулярно проводить антивирусное сканирование.*

Источник: Следственный комитет Республики Беларусь.

При оплате товаров в интернете:

- используйте для платежей отдельную карту;

- переводите на указанную карту точную сумму денежных средств, которая необходима вам для оплаты;

- производите оплату только с устройств (ноутбуков, планшетов, компьютеров, мобильных телефонов), защищенных антивирусным программным обеспечением*;

- не используйте для расчетов устройство, к которому имеют доступ более одного человека;

- в настройках используемого браузера нужно запретить сохранение логинов, паролей и другой конфиденциальной информации;

- при работе на устройстве, с которого производится оплата, ни в коем случае не переходите по сомнительным ссылкам;

- после завершения сеанса оплаты рекомендуется выйти из браузера.

*Антивирус должен быть включен, антивирусные базы и программа - обновляться, следует регулярно проводить антивирусное сканирование.

Источник: Следственный комитет Республики Беларусь.

ИНФОГРАФИКА
09 АПРЕЛЯ 2021, 14:14

Как не стать жертвой вишинга

КАК НЕ СТАТЬ ЖЕРТВОЙ ВИШИНГА

Вишинг (голосовой фишинг - voice fishing) - один из методов мошенничества с использованием социальной инженерии. Злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию (ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды) или стимулируют к совершению определенных действий со своим карточным счетом/платежной картой.

Вам позвонили/прислали СМС "из банка" с неизвестного номера:

- не торопитесь следовать инструкциям;
- не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;
- проверьте информацию, позвонив в контактный центр банка;
- незамедлительно обратитесь в правоохранительные органы.

Вам позвонили/прислали СМС с неизвестного номера с просьбой о помощи близкому человеку:

- не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей;
- задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;
- под любым предлогом постарайтесь прервать контакт с собеседником, позвоните родным и узнайте, все ли у них в порядке.

Вы заподозрили интернет-продавца в недобросовестности:

- необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки;
- никогда не переводите деньги незнакомым людям в качестве предоплаты.

Источник: Следственный комитет Республики Беларусь.

Вишинг - один из методов мошенничества с использованием социальной инженерии. Злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию (ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды) или стимулируют к совершению определенных действий со своим карточным счетом/платежной картой.

Вам позвонили/прислали СМС "из банка" с неизвестного номера:

- не торопитесь следовать инструкциям;

- не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;

- проверьте информацию, позвонив в контактный центр банка;

- незамедлительно обратитесь в правоохранительные органы.

Вам позвонили/прислали СМС с неизвестного номера с просьбой о помощи близкому человеку:

- не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей;

- задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;

- под любым предлогом постарайтесь прервать контакт с собеседником, позвоните родным и узнайте, все ли у них в порядке.

Вы заподозрили интернет-продавца в недобросовестности:

- необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки;

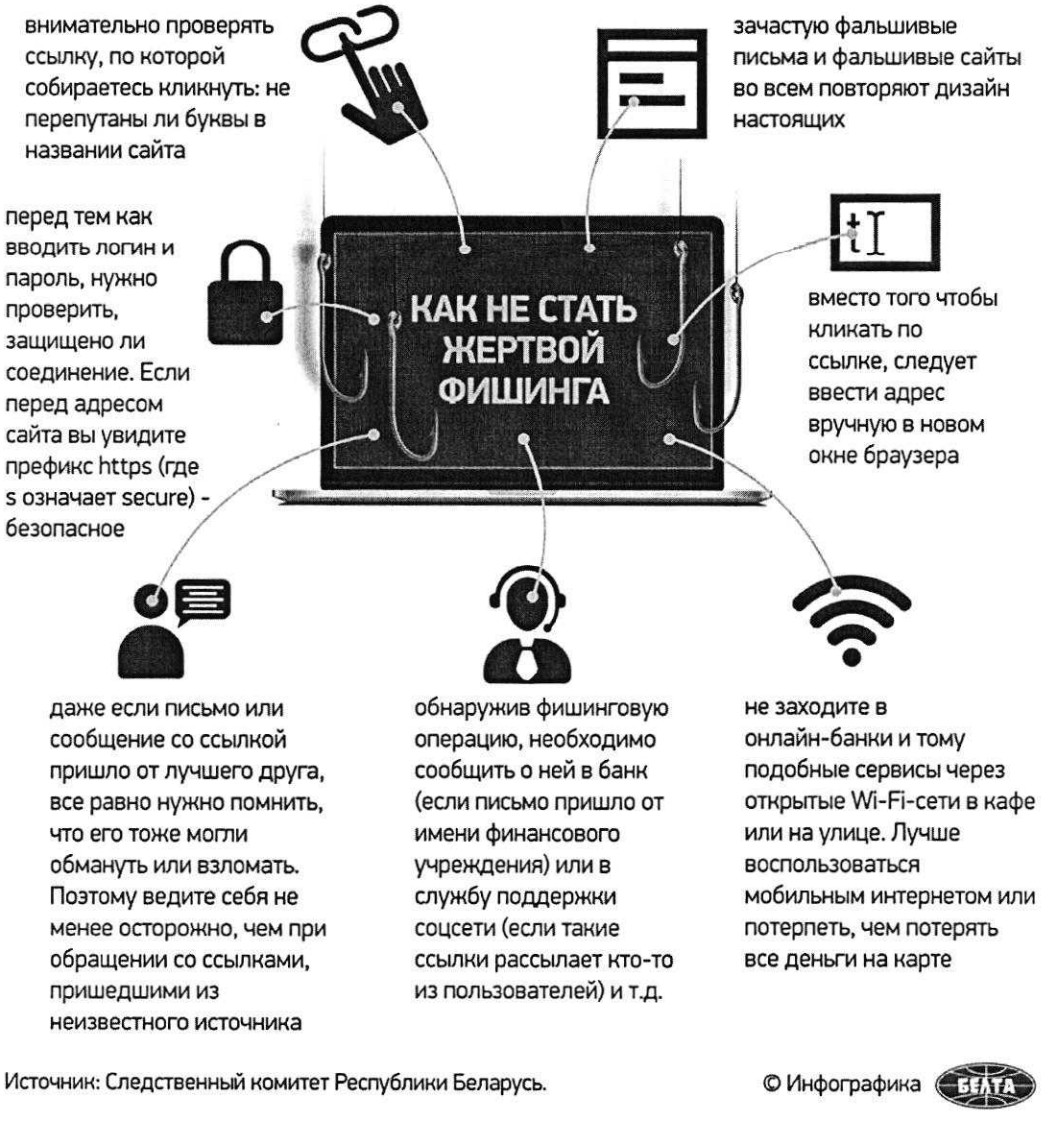
- никогда не переводите деньги незнакомым людям в качестве предоплаты.

Источник: Следственный комитет Республики Беларусь.

Вы можете найти эту страницу по следующему адресу:
https://www.belta.by/infographica/view/kak-ne-stat-zhertvoj-vishinga-24468/

КАК НЕ СТАТЬ ЖЕРТВОЙ ФИШИНГА

Фишинг (англ. phishing от fishing "рыбная ловля, выуживание") - вид интернет-мошенничества для получения доступа к конфиденциальным данным пользователей - логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков или внутри социальных сетей.



Источник: Следственный комитет Республики Беларусь.

Фишинг (англ. phishing от fishing "рыбная ловля, выуживание") - вид интернет-мошенничества для получения доступа к конфиденциальным данным пользователей - логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков или внутри социальных сетей.

Как не стать жертвой фишинга:

- внимательно проверять ссылку, по которой собираетесь кликнуть: не перепутаны ли буквы в названии сайта;

- перед тем как вводить логин и пароль, нужно проверить, защищено ли соединение. Если перед адресом сайта вы увидите префикс https (где s означает secure) - безопасное;

- даже если письмо или сообщение со ссылкой пришло от лучшего друга, все равно нужно помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника;

- зачастую фальшивые письма и фальшивые сайты во всем повторяют дизайн настоящих;

- вместо того чтобы кликать по ссылке, следует ввести адрес вручную в новом окне браузера;

- обнаружив фишинговую операцию, необходимо сообщить о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки соцсети (если такие ссылки рассылает кто-то из пользователей) и т.д.;

- не заходите в онлайн-банки и тому подобные сервисы через открытые Wi-Fi-сети в кафе или на улице. Лучше воспользоваться мобильным интернетом или потерпеть, чем потерять все деньги на карте.

Источник: Следственный комитет Республики Беларусь.

Вы можете найти эту страницу по следующему адресу:
https://www.belta.by/infographica/view/kak-ne-stat-zhertvoj-fishinga-24467/