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.

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

зачастую фальшивые письма и фальшивые сайты во всем повторяют дизайн настоящих

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

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

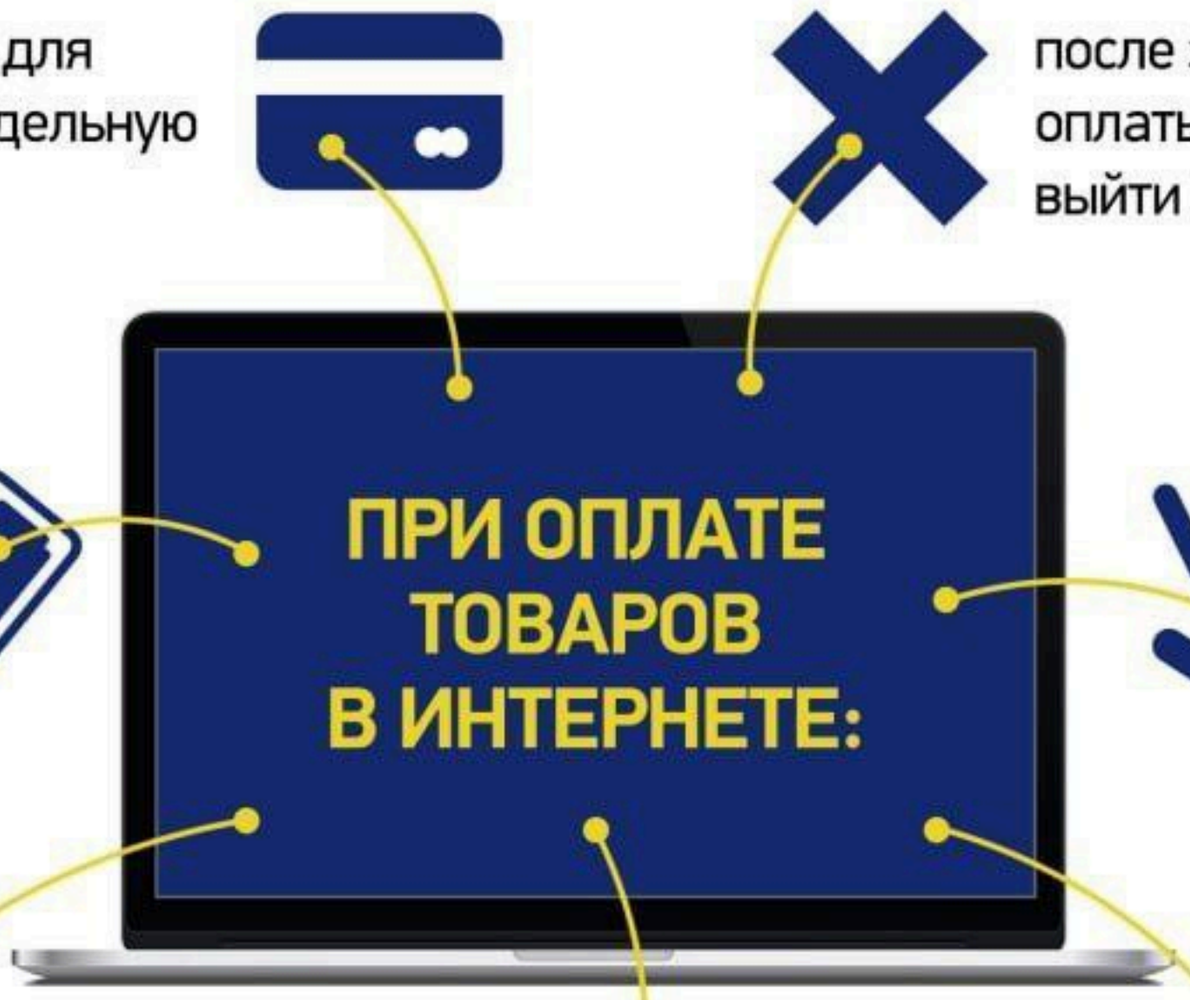
даже если письмо или сообщение со ссылкой пришло от лучшего друга, все равно нужно помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника

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.

КАК НЕ СТАТЬ ЖЕРТВОЙ ИНТЕРНЕТ-МОШЕННИКОВ



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*

после завершения сеанса оплаты рекомендуется выйти из браузера

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

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

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

Источник: Следственный комитет Республики Беларусь.

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.

Милиция Минска предупреждает

ОСТОРОЖНО! МОШЕННИКИ!

...Недавно столичная пенсионерка дважды доверилась мошенникам: преступники **смогли выманить 50 тысяч BYN**

ЖЕНЩИНА ОТВЕТИЛА НА ОБЪЯВЛЕНИЕ О «ВЫПЛАТАХ НАСЕЛЕНИЮ» И ВСКОРЕ ПОЛУЧИЛА ЗВОНОК ОТ «КОНСУЛЬТАНТА», КОТОРЫЙ РАССКАЗАЛ, КАК ЗАРАБОТАТЬ ДЕНЬГИ ЧЕРЕЗ ТОРГОВЛЮ НА БИРЖЕ.

ЕСЛИ ВАМ ПРЕДЛАГАЮТ ПОДЗАРАБОТАТЬ НА БИРЖЕ, ПОМНИТЕ:

1. Если проект обещает невероятно высокие проценты или быструю прибыль - **это должно насторожить.**
2. Если куратор настоятельно требует **принять решение быстро** или угрожает потерями - это тоже может быть признаком мошенничества.
3. Неоднократные **требования пополнения счета** или перевода средств на сторонние счета - плохой знак!
4. Просьбы **установить на телефон "специальные программы"** и внести предоплату - красный флаг!

Советы, которые помогут не попасться на удочку мошенников:

- **Прежде чем инвестировать деньги куда-либо** или переходить по ссылкам, **всегда проверяйте информацию.**
- **Избегайте слишком хороших предложений** и обещаний быстрой прибыли.
- **Никогда не инвестируйте больше,** чем можете позволить себе потерять.
- Если сомневаетесь в безопасности действий, лучше **позвоните по номеру 102.**

Милиция Минска

БУДЬ КИБЕРГЕРОЕМ!

Будь как ниндзя!
Не сообщай незнакомым людям в Интернете свое настоящее имя, адрес и номер телефона.
Будь осторожен с тем, что пишешь о себе.

Придумай сложный пароль, как у супергероя!
Никому его не говори, ведь это твой секретный ключ!

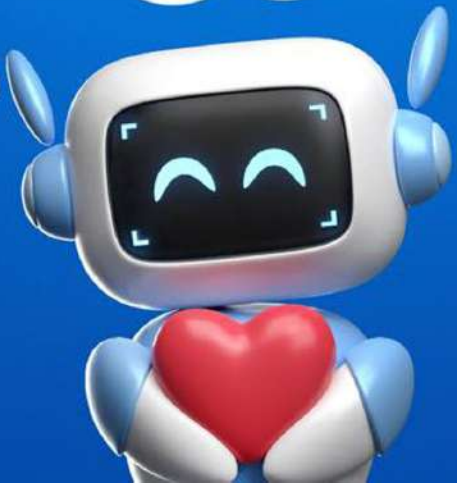
Помни, что в Интернете не все те, кем кажутся!
Не добавляй в друзья людей, которых не знаешь в реальной жизни.

Будь как хакер!
Не кликай на подозрительные ссылки.

Будь осторожен, как на минном поле!
Скачивай приложения только из официальных магазинов.
Антивирус - твой верный друг!

Не бойся просить о помощи!
Если тебя что-то тревожит в Интернете, расскажи об этом родителям или учителю.
Вместе вы сможете решить любую проблему.

Интернет - это круто, но помни о безопасности!
Соблюдая эти правила, ты сможешь стать настоящим кибергероем!



МУС

mvd.gov.by

ЛЖЕБЕЛТЕЛЕКОМ

1 Вам звонят якобы из Белтелекома и требуют срочно продлить договор на ТВ или интернет. Для этого просят назвать номер паспорта.

2 Затем перезванивает якобы "сотрудник правоохранительных органов" и говорит, что вас пытались обмануть, а ваши данные уже используются в преступных целях.

3 Далее вас запугивают обыском и убеждают задекларировать наличные через Национальный банк или просят передать деньги курьеру по кодовому слову.

4 Курьер приходит, забирает деньги, и вы их больше не увидите.

Не хотите быть обманутым ? — Немедленно положите трубку!

ПОМНИТЕ:

- Договоры с Белтелекомом бессрочные, по телефону не продлеваются;
- Все звонки — только с белорусских номеров, НИКОГДА через мессенджеры;
- Сотрудники компании не запрашивают личные данные по телефону, а только при ЛИЧНОМ обращении в офис.

Если вы стали жертвой преступления или получили такой звонок – немедленно позвоните в милицию по телефону «102»!

УПК КМ ГУВД МИНГОРИСПОЛКОМА

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:

Получить кредит, чтобы отменить якобы оформленный неизвестными на ваше имя другой кредит и перевести деньги на специальный счет

Установить программное обеспечение, якобы для предотвращения мошеннической атаки на ваш счет

Перевести накопления на якобы безопасный счет, чтобы не изъяли при обыске

Передать личные данные и код из смс, такие сведения предоставляют мошенникам доступ к счету или сервису

ОСТОРОЖНО! МОШЕННИЧЕСТВО!

В СОЦИАЛЬНЫХ СЕТЯХ И НА ТОРГОВЫХ ПЛОЩАДКАХ:

Перевести предоплату за несуществующий товар в лжемагазине или по измененным реквизитам банка

Перейти по поддельной ссылке банковской системы и ввести личные данные (логин и пароль, номер и трехзначный код с оборотной стороны банковской карты, код из СМС, кодовое слово)

Перечислить деньги на карту или оплатить родственнику, другу, любящему человеку

На поддельной бирже вложить деньги в проект, якобы для получения пассивного дохода

МОШЕННИКИ УБЕЖДАЮТ,
представляясь продавцами, друзьями, партнерами по бизнесу, руководителями инвестиционных проектов

Больше информации на сайте https://mvd.gov.by

Главное управление по противодействию киберпреступности КМ МВД Республики Беларусь

Законные сделки с криптовалютой

Убедитесь, что Ваши сделки соответствуют действующему законодательству Республики Беларусь

Порядок осуществления сделок с криптовалютой определен Декретом Президента Республики Беларусь от 21 декабря 2017 г. №8 «О развитии цифровой экономики» и Указом Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)»

В Республике Беларусь физическим лицам:

РАЗРЕШЕНО

Добыча криптовалюты в результате майнинга
(как на территории Республики Беларусь, так и на территории иностранного государства)

Продажа (покупка) криптовалюты за денежные средства на белорусских криптоплатформах, являющихся резидентами Парка высоких технологий

Обмен криптовалюты на иные токены
(на белорусских и иностранных криптоплатформах)

Получение криптовалюты в дар или наследство

ЗАПРЕЩЕНО

Продажа (покупка) криптовалюты за денежные средства на иностранных криптоплатформах

Продажа (покупка) криптовалюты за денежные средства напрямую между физическими лицами

БОЛЬШЕ ИНФОРМАЦИИ

В Telegram-канале
КИБЕРКРЕПОСТЬ
CYBER_FORTRESS_BREST

КИБЕРКРЕПОСТЬ

Главное управление по противодействию киберпреступности
КМ МВД Республики Беларусь

Привет! Я бот ScamBY!

Найду свет в темноте, подсвечу опасность!

- Проверка сайтов
- Проверка Instagram
- Проверка Telegram
- Проверка TikTok

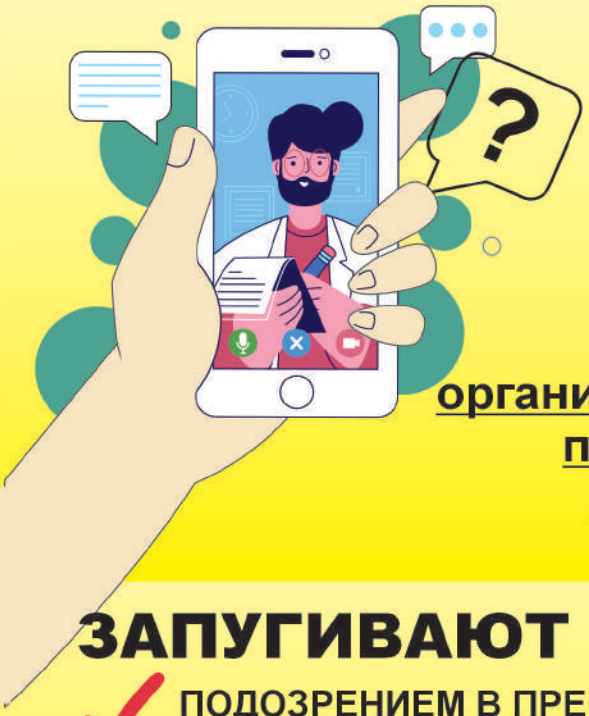
Отправь ссылку или имя аккаунта – проверю ресурс на мошенничество!

БЕЛАРУСЬ

Попробуй прямо сейчас!

Проверь ресурс с ScamBY!

@SCAMBY_BOT



ТЕЛЕФОННЫЕ МОШЕННИКИ

представляются работниками:
<u>коммунальных служб</u>
(энергонадзора, водоканала, газовой службы),
<u>организаций связи</u> (Белтелеком, Белпочта, МТС, А1),
<u>правоохранительных органов и банков</u>
<u>продавцами, инвесторами, брокерами</u>

ЗАПУГИВАЮТ ИЛИ ЗАВЛЕКАЮТ:

- ✓ ПОДОЗРЕНИЕМ В ПРЕСТУПЛЕНИИ, ПРОВЕДЕНИЕМ ОБЫСКА
- ✓ СЛОЖНОЙ СИТУАЦИЕЙ С РОДСТВЕННИКОМ
- ✓ БЫСТРЫМ ЗАРАБОТКОМ И ПОЛУЧЕНИЕМ ПРИБЫЛИ
- ✓ ОКОНЧАНИЕМ ДЕЙСТВИЯ ПРИБОРА УЧЕТА
- ✓ ОКОНЧАНИЕМ ДЕЙСТВИЯ ДОГОВОРА ИЛИ УСЛУГИ СВЯЗИ
- ✓ ДЕЙСТВИЕМ АКЦИЙ, СКИДОК, ПРОВЕДЕНИЕМ РОЗЫГРЫШЕЙ

УБЕЖДАЮТ:

- ОФОРМИТЬ «ВСТРЕЧНЫЙ» КРЕДИТ
- СООБЩИТЬ ЛИЧНЫЕ ДАННЫЕ И КОД ИЗ УВЕДОМЛЕНИЯ
- ВНЕСТИ ПРЕДОПЛАТУ ЗА ТОВАР ИЛИ УСЛУГ
- ПЕРЕВЕСТИ ДЕНЬГИ НА «БЕЗОПАСНЫЙ» СЧЕТ
- СКАЧАТЬ И УСТАНОВИТЬ ФАЙЛ ПРИЛОЖЕНИЯ (*.APK)
- ВНЕСТИ СУММУ НА СЧЕТ ДЛЯ НАЧАЛА ИНВЕСТИРОВАНИЯ

✓ УБЕДИТЕСЬ В ДОСТОВЕРНОСТИ ЗВОНКА

ПО ДРУГИМ КАНАЛАМ СВЯЗИ

Главное управление
по противодействию
киберпреступности
МВД Республики Беларусь