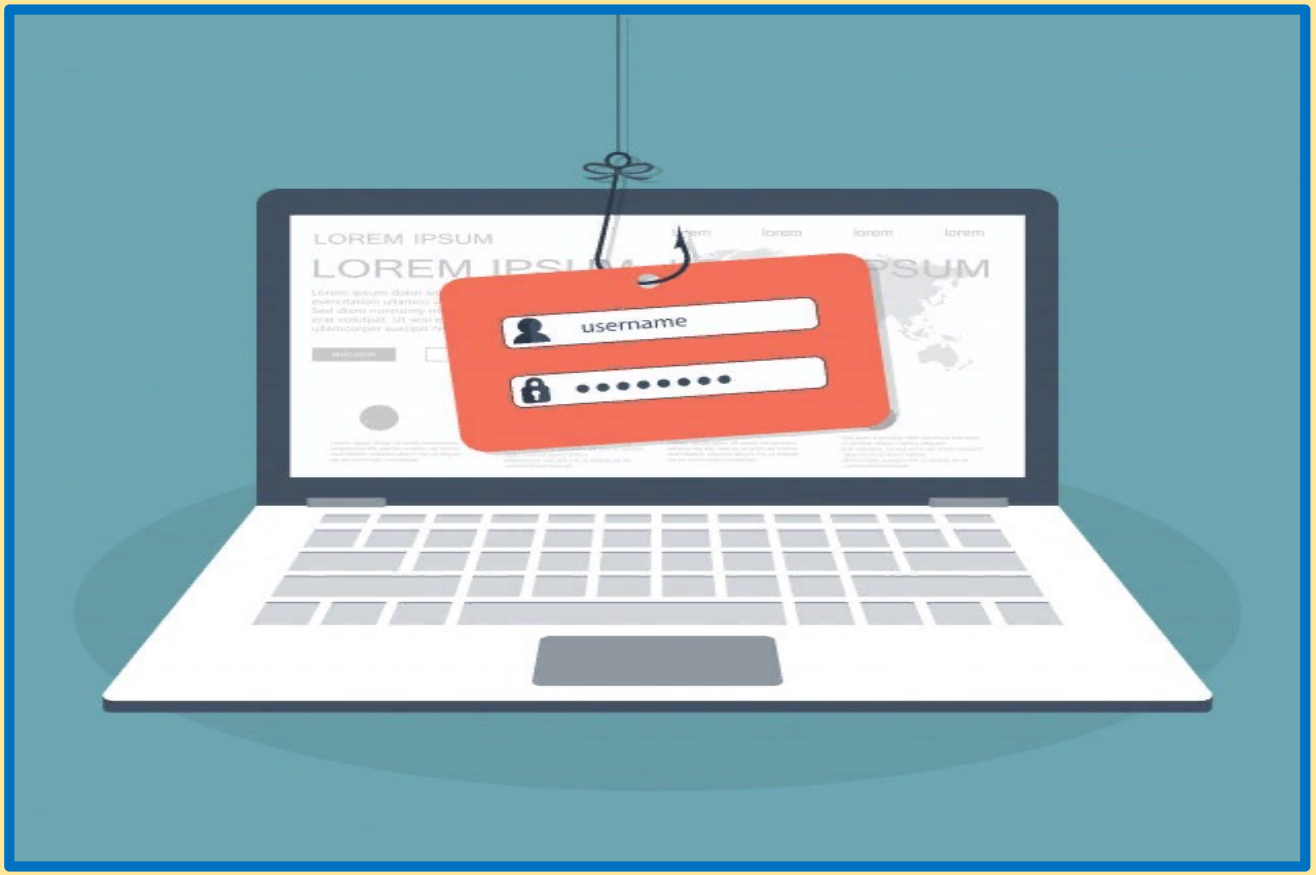
Финансовая грамотность

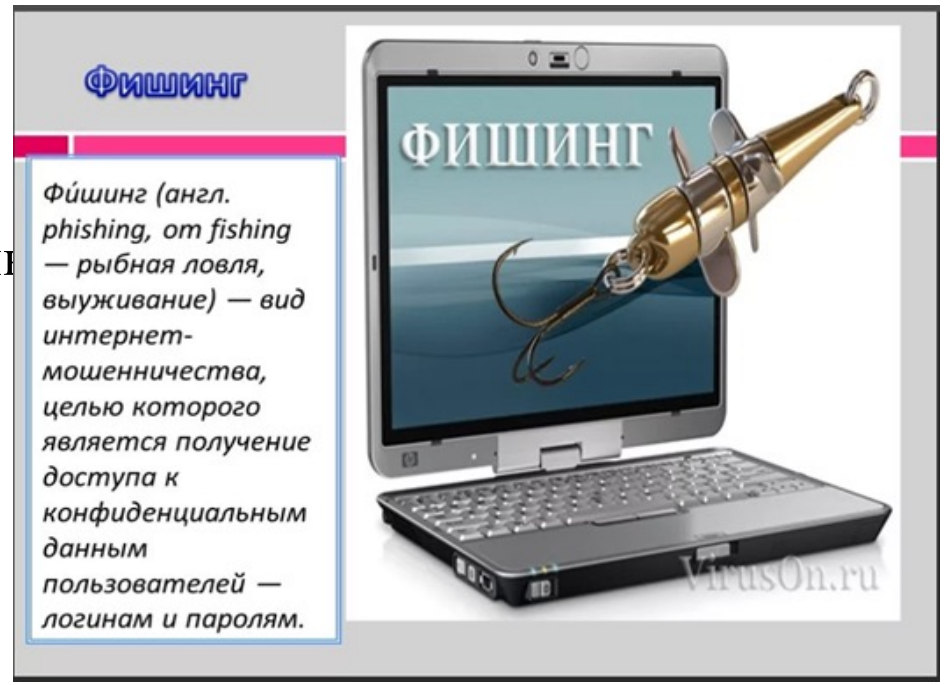
Фишинг: что это такое и как от него защититься



Актуальность темы: за свое короткое существование Интернет стал основным средством коммуникации.

Диапазон пользователей – очень большой. Пользователями интернета могут быть как и 10-ти летние, наивные и глупые дети, так и опытные пользователи с 15-летним стажем. Первый вид или близкие к ним пользователи, на данный, момент наиболее распространен, поэтому обманывать сейчас очень легко.

Видов мошенничества также очень много, от самых примитивных и банальных до весьма продуманных.



Цель занятия:

Ознакомиться с видами мошенничества.

Научить пользователей не вестись на эти обман

Задачи:

Изучить виды мошенничества.

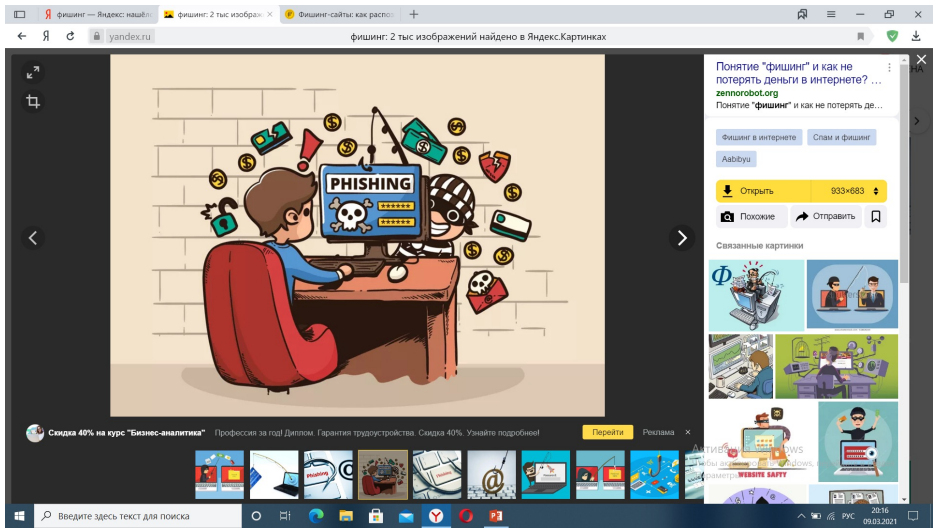
Изучить меры предосторожности.

ТИПИЧНАЯ СИТУАЦИЯ.

Николай получил электронное письмо от интернет-магазина, в котором часто делает покупки: «Подтвердите свой аккаунт, чтобы продолжать пользоваться бонусами».

Николай перешел по ссылке из письма, заново ввел свои личные данные и данные банковской карты. Затем его попросили сделать «пробный платеж» на 1 рубль. В ходе оплаты надо было ввести трехзначный код с обратной стороны карты. Как только Николай ввел этот код, ему пришло сообщение от банка о списании со счета, но вовсе не 1 рубля,

а 10 000 рублей.



Разбираемся, как так получилось.

На самом деле письмо Николаю прислал не магазин, а кибермошенники. Они обманом выманили у Николая конфиденциальные данные, и он даже не заметил, как попался на их удочку. **Этот вид мошенничества так и называется — фишинг.** То есть рыбалка, ловля на крючок.

Обычно преступники сначала цепляют человека за живое: запугивают потерей денег или завлекают супервыгодой, пробуждают любопытство или сочувствие. Затем выманивают личные данные, реквизиты счета или карты. И в итоге списывают деньги с банковского счета.

Рассмотрим, какие ошибки допустил Николай и как он мог защититься от потери денег.

Рассмотрим, какие ошибки допустил Николай и как он мог защититься от потери денег.

Ошибка № 1: не использовать антивирусную защиту

Николай считал пустой тратой денег покупку антивируса. Он решил, что гораздо проще и дешевле самому чистить почтовый ящик от спама.

Как устранить ошибку

На все свои гаджеты — компьютер, ноутбук, планшет и смартфон — нужно установить антивирус. Хороший антивирусный пакет включает защиту от спама и фишинговых писем. Он сам распознает подозрительных адресатов.

Кроме того, антивирус защитит от программ, которые воруют данные карт, получают доступ к онлайн- и мобильным банкам, перехватывают СМС и push-сообщения с секретными кодами. Это еще опаснее, чем фишинг, — ваш счет могут обнулить, а вы об этом даже не сразу узнаете.

Важно регулярно обновлять защиту. Кибермошенники изобретают новые вирусы и способы фишинга буквально каждый день.

Ошибка № 2: переходить по ссылкам из сообщений от незнакомых адресатов

Николай решил, что получил письмо от онлайн-магазина — он увидел знакомое название и логотип в тексте письма. Но адрес отправителя он не проверил.

Как действуют преступники

Мошенники регистрируют адрес почты, похожий на адрес реального интернет-магазина, банка или другой легальной организации. Например, вместо настоящего адреса магазина «Супершоп» mail@supershop.ru используют mail@supersshope.ru.

Иногда обманщики даже не заморачиваются с похожим адресом, так как зачастую он скрыт от глаз пользователя. Просто указывают название магазина как имя отправителя — именно его и видит получатель. Подмену проверить легко, но не все обращают внимание на такие детали.

Мошенники заманивают людей на фишинговые сайты не только через электронную почту, но и через мессенджеры и социальные сети. Вам может прийти сообщение от знакомого, который предлагает перейти по ссылке. Но может оказаться, что его аккаунт взломали.

Иногда преступники даже не стараются мимикрировать под кого-то другого. Вместо этого они запускают свой собственный бизнес-проект. И создают видимость, что проводят викторины с гарантированным выигрышем, анкетирование за вознаграждение или рассылают видео для взрослых.

В текст письма или сообщения они добавляют ссылку, которая вместо обещанных викторин и видео ведет на фишинговый сайт. Его создают специально для этой аферы, чтобы собирать личные и платежные данные пользователей. В некоторых случаях при переходе по ссылке загружается вирус, который ворует данные с вашего устройства.

Обманщики подбирают тему письма, на которую получатель должен среагировать. Что-то пугающее: «Ваш аккаунт будет заблокирован», «Срочное сообщение от Службы безопасности». Или завлекающее: «Вам начислено 3000 бонусов», «Возврат платежа на 12 000 рублей». Или интригующее: «Привет! Шлю тебе фотки с последней вечеринки». Мошенники умеют играть на эмоциях.

Как избежать уловок мошенников

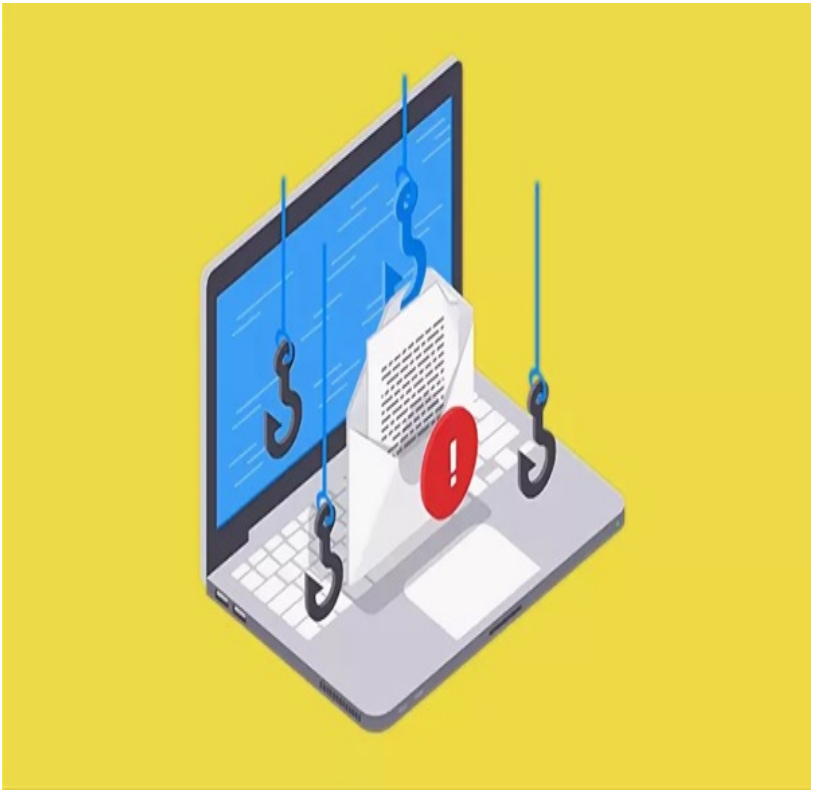
Всегда тщательно проверяйте адрес, с которого пришло письмо. Если он хотя бы одним символом отличается от привычного адреса магазина, банка, авиакомпании или другой реальной организации, такое письмо не стоит даже открывать. Если же адрес вам вообще не знаком и вы не ждете сообщений от новых адресатов, то можете смело его удалять.

Когда откроете письмо, обратите внимание на то, как оно написано и оформлено. Орфографические ошибки и ужасный дизайн — явный признак поддельного письма. Но в последнее время мошенники научились очень точно повторять фирменный стиль известных компаний. Так что стоит быть внимательным, даже если все выглядит идеально.

Если непонятную ссылку прислал друг или знакомый, лучше перезвонить и удостовериться, что это сообщение точно от него.

Ошибка № 3: не проверять адресную строку сайта

- Николай заметил, что привычный дизайн интернет-магазина немного изменился, но это его не насторожило. Внимательно изучить адресную строку браузера ему и в голову не пришло.



Что нужно проверять при переходе на сайт

Адрес. Лучше всего сохранять адреса банков, госорганов, любимых интернет-магазинов и других онлайн-сервисов в закладках. Можно вбивать адрес вручную, но нужно быть внимательным — иногда ошибка даже в одном символе приведет вас на фишинговый сайт-двойник.

Всегда проверяйте адресную строку браузера. Иногда можно попасть на фишинговый сайт даже при переходе с одной страницы известного вам портала на другую.

Безопасность соединения. Если вы хотите ввести персональную информацию или данные карты, сделать покупку через сайт, то перед его адресом обязательно должно стоять https и значок закрытого замка. Буква s и закрытый замок означают, что соединение защищено: когда вы вводите на сайте данные, они автоматически шифруются и их не могут перехватить.

Защищенное соединение — требование обязательное, но не достаточное. Хакеры не могут подключиться к такому сайту и узнать ваши данные. Но это не гарантия того, что сам сайт создан законопослушной компанией. В последнее время и преступники умудряются получать сертификаты безопасности для своих сайтов.
Дизайн. Даже если вы проморгали лишнюю букву в адресе, а преступники организовали защищенное соединение, плохой дизайн сайта должен броситься в глаза.

Преступники создают онлайн-ресурсы с простой целью — собрать конфиденциальные данные. Поэтому в большинстве случаев они не мудрят со структурой и дизайном сайта. Небрежная верстка, орфографические ошибки, неработающие разделы и ссылки — явные признаки фальшивки.
Но если у мошенников большие амбиции, они могут вложиться в создание сайта, который максимально точно повторяет интернет-ресурс известной организации. Или создать красивый и качественный сайт своего собственного «проекта». Так что только на дизайн тоже ориентироваться нельзя.

Ошибка № 4: платить через небезопасные страницы

Фальшивый «интернет-магазин» предложил Николаю провести «пробный платеж» и для этого ввести код с обратной стороны карты и код из СМС-сообщения прямо на своем сайте. Николай не обратил внимания, что для проведения оплаты его не перекинули на страницу платежной системы.

Что нужно знать

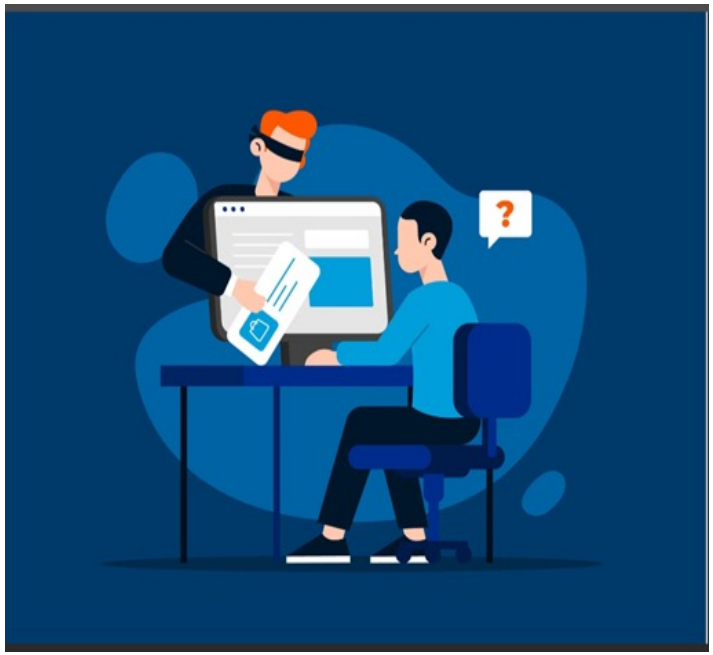
После ввода реквизитов карты сайт магазина должен перекинуть вас на шлюз платежной системы вашей карты. Это отдельная безопасная страница, интернет-магазин не может получить доступ к информации, которую вы там введете.

Платежные шлюзы соединяют владельца карты с его банком при проведении платежа. Банк присылает клиенту в СМС-сообщении одноразовый код для подтверждения операции. И только после того, как покупатель его вводит, проходит платеж.

Никому не сообщайте секретные коды от банка — проверьте, совпадают ли данные из СМС с деталями операции. Если все в порядке, вбейте код в специальное поле на странице оплаты. Если нет — позвоните в банк.

Безопасные шлюзы есть у всех платежных систем. Ищите их логотипы на странице оплаты: Visa Secure, MasterCard SecureCode и Mir Accept. Причем логотипы должны быть активными ссылками, которые ведут на сайты платежных систем. На страницах мошенников эти логотипы — просто картинки.

Ошибка № 5: использовать одну и ту же карту для всех платежей



Николай платил в интернет-магазинах своей зарплатной картой. Теперь ему придется заказать новую. А пока банк будет ее перевыпускать, доступ к остатку денег на счете он сможет получить только в отделении банка.

Как стоит поступать

Для онлайн-покупок и оплаты услуг через интернет лучше завести отдельную карту. Стоит переводить на нее деньги прямо перед платежом и класть ровно ту сумму, которую собираетесь перечислить.

Некоторые банки и системы электронных платежей (электронные кошельки) предлагают заводить виртуальные карты — у них есть реквизиты, но в виде пластика они не существуют. Иногда можно даже создавать виртуальные карты, которые действительны лишь для одной онлайн-покупки.

Правовая оценка фишинга.

Создание фишингового сайта можно квалифицировать по ст. 180 УК РФ «Незаконное использование товарного знака».

В данном случае злоумышленники с целью введения жертвы в заблуждение используют чужие товарные знаки, знаки обслуживания и другие средства индивидуализации при создании фишинговых сайтов, делая их схожими до степени смешения с оригинальными товарными знаками, размещенными на официальных сайтах их легальных правообладателей.

Информационные ресурсы

1. https://fincult.info/article/fishing-chto-eto-takoe-i-kak-ot-nego-zashchititsya/
2. https://fincult.info/
3. https://fincult.info/article/chto-delat-esli-vashi-prava-narusheny/
4. http://www.cbr.ru/