ФИШИНГ

Работу выполнили
ученицы 11БК класса
Щербакова Вика и
Коптева Полина

- Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей.

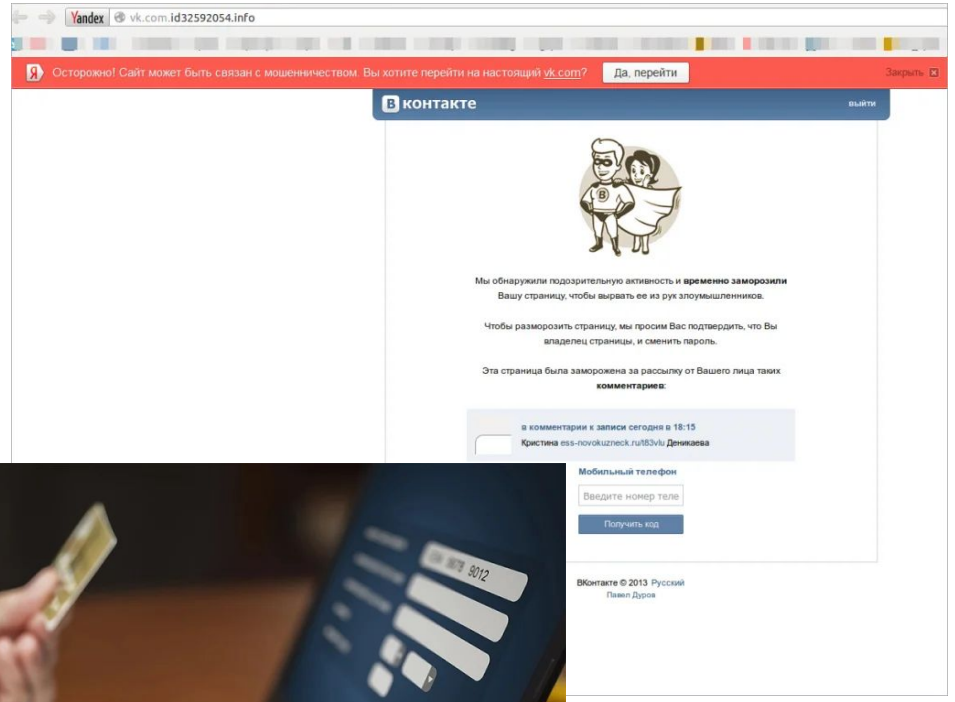
КАК РАБОТАЕТ ИНТЕРНЕТ-ФИШИНГ?

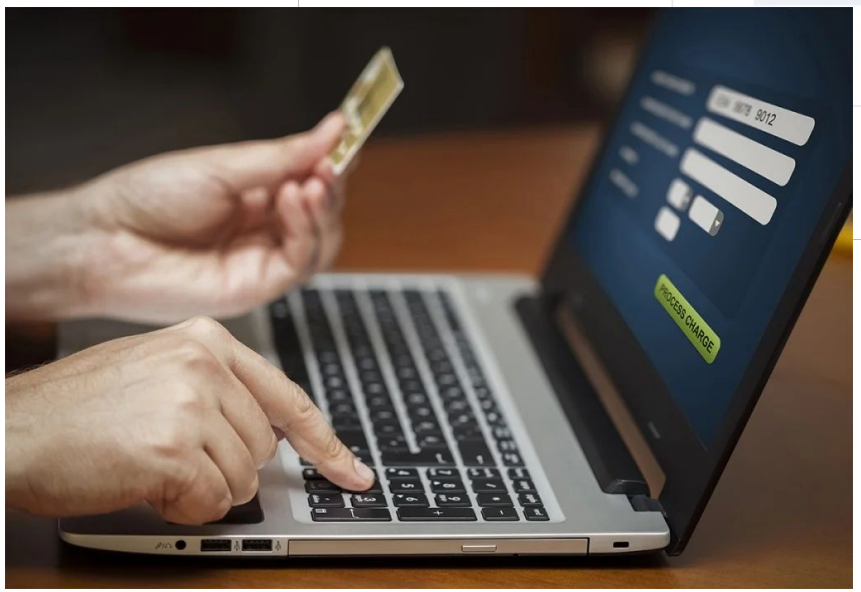
- Жертва, ничего не подозревая, сама предоставляет все личные данные. Используя всплывающие окна, таргетированную рекламу или вирусные landingpage, фишеры выманивают любую информацию.
- Низкий уровень осведомленности пользователей позволяет с мошенникам с легкостью получать доступ к любым персональным данным. Вирусным атакам могут подвергаться не только единичные пользователи, но и крупные компании, банки или платежные системы.

- В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

КАК ОПРЕДЕЛИТЬ ФИШИНГОВЫЙ САЙТ?

- Визуальная проверка сайтов. (например, «http», а не «https»; адрес «vcccom.ru» вместо правильного «vk.com»)
- Регистрация на сайте с помощью указания данных банковских карт или логина и пароля от почты.
- Так же при оплате интернет-покупок картой на сайте нужно следить за тем, маскируются ли реквизиты (например, CVC-код)





КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА?

- Чтобы знать, как бороться с фишинговыми сайтами, необходимо иметь минимальные знания об интернете, его использовании и методах защиты информации. Чтобы не попасть на уловки, помните несколько правил:

- не передавайте конфиденциальные данные;
- установите антивирус;
- обращайте внимание на оформление;
- проверяйте правильность ссылки в адресной строке;
- пользуйтесь защищенным соединением https;
- фильтруйте подозрительные письма;
- не пользуйтесь открытыми точками доступа wi-fi для входа в банковские аккаунты.