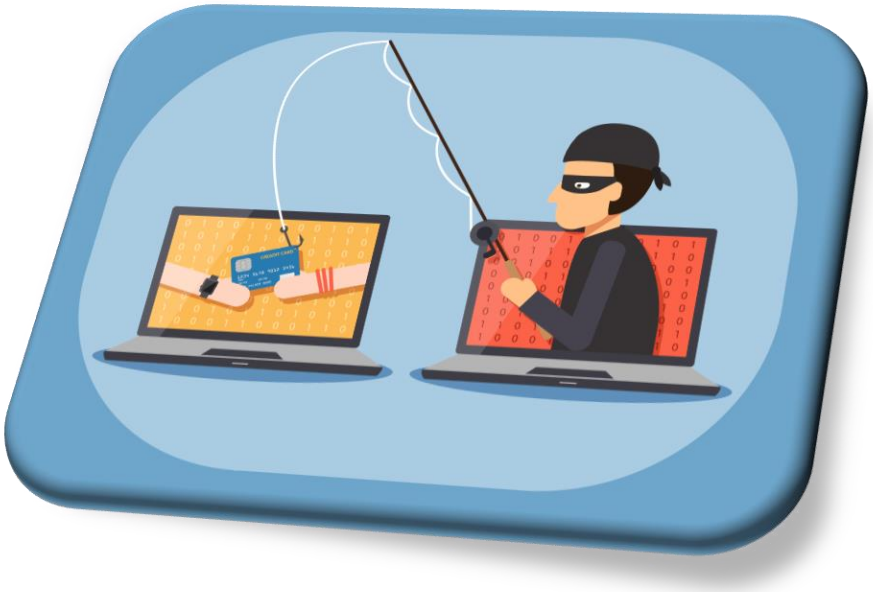


ИНТЕРНЕТ БЕЗОПАСНОСТЬ

ЧТО ТАКОЕ ФИШИНГОВАЯ ССЫЛКА/САЙТ?

Фишинговая ссылка

— это адрес веб-страницы, на которой мошенники крадут конфиденциальную информацию, оставленную посетителем. Например, логины и пароли от банковских карт.

Сам фишинг является видом социальной инженерии, с помощью которой «жертву» побуждают к действиям, выгодным злоумышленникам.

Особое внимание обратим на фишинг в социальных сетях

Мошенники всеми путями стараются заполучить логин и пароль от аккаунта «жертвы», особенно это актуально для социальных сетей.

3 самых популярных вида фишинга:

Почтовый — когда мошенники выдают себя за какие-то известные компании. Электронный адрес которых визуально схож с их email;

Смишинг — отправка СМС-сообщений с вредоносной ссылкой;

«Злой двойник» - создается копия официальной сети WiFi, при подключении к ней жертву перебрасывают на фишинговый сайт

ГОРОДСКОЙ ПСИХОЛОГО-ПЕДАГОГИЧЕСКИЙ ЦЕНТР ДЕПАРТАМЕНТА ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ

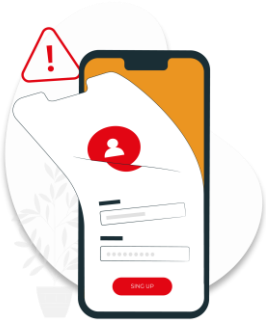
Есенинский бульвар, д. 12, к. 2
Единая справочная:
8 495 730 2193
E-mail: gppc@edu.mos.ru

ГОРОДСКОЙ ПСИХОЛОГО-ПЕДАГОГИЧЕСКИЙ ЦЕНТР ДОНМ

Романтическое знакомство — вы общаетесь с симпатичным парнем или девушкой. В какой-то момент под «красивым» предлогом вас просят перейти по ссылке. После этого взламывают аккаунт

Лотереи. Приходит сообщение, что вы выиграли деньги. Нужно только перейти по ссылке, чтобы их забрать. Дальше, либо взломают аккаунт, либо сделают еще какую-нибудь пакость

Спонсорство инфлюенсеров. Мошенники предлагают рекламную сделку от имени крупной компании или популярного блогера. На деле же у вас выманивают банковские реквизиты



Розыгрыш призов. В обмен на какой-нибудь бонус вас просят перевести маленькую сумму денег, чтобы убедиться в вашей честности. Надо ли говорить, что ни приза, ни возврата денег вы не получите?

Фишинговые письма. На почту «прилетает» предупреждение о том, что в вашем аккаунте ведется подозрительная активность, поэтому надо перейти по ссылке и зайти в профиль. Как только вы это сделаете, лишитесь доступа к своей странице в социальных сетях

ДРУГИЕ ВИДЫ ФИШИНГА:

Фишинг в поисковиках — мошенник создает сайт с дешевыми товарами, поисковые системы его индексируют, жертва переходит по адресу, и под разными предлогами у нее выманивают данные банковской карты

Клон-фишинг — ранее доставленное письмо от настоящего отправителя копируется, ссылки заменяются вредоносными, адрес подделывается, в теме письма говорится, что в старом забыли добавить важные элементы

CEO-мошенничество — получение доступа к аккаунту электронной почты руководителя для отправки писем сотрудникам компании, чтобы те выполнили какие-то нужные злоумышленнику действия

Вишинг — атака, во время которой у человека по телефону выманивают какие-то ценные данные, часто используется персональная информация о жертве

Фарминг — в этом случае жертву скрытно перенаправляют на ложный IP-адрес. Человек открывает сторонний файл или вредоносное письмо. После этого на компьютер «проникает» вирус, «заражает» систему, но при этом находится в спящем режиме, поэтому его не замечает ни один антивирус. Дальше пользователь заходит в свои аккаунты в банках или платежных системах. Вирус «оживает» и сразу перенаправляет юзера с оригинального сайта на поддельный. Человек ничего не замечает, а мошенники получают его персональные данные или деньги

Самое главное правило — не переходить по ссылкам из писем от незнакомых пользователей. Также не следует переходить по коротким ссылкам типа bit.ly или goo.gl, даже если они от друзей: их аккаунты могли взломать. На компьютере всегда должен стоять антивирус с обновленными базами данных.