Минцифра Оренбургской области
digital.orb.ru

Как не стать жертвой взлома через фишинг?

Важные рекомендации от нашего центра кибербезопасности

Фи́шинг (англ. phishing от fishing «рыбная ловля, выуживание») *— вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.*

Подозрение на фишинг должны вызывать письма, которые побуждают Вас выполнить какое-либо действие, как правило перейти по ссылке. Далее может быть форма авторизации или вполне легитимное содержимое с которым может произойти вирусное заражения вашего устройства.

Каждое письмо от любого отправителя может быть фишинговым.

Если вы с коллегой или организацией переписывались достаточно долго, это ни в коей мере не означает, что следующее письмо от этого отправителя не будет фишинговым.

Вашего коллегу или партнера могли взломать и воспользоваться его статусом

Злоумышленник мог подменить адрес отправителя, что бы выдать себя за него

Что делать?

Если в письме есть ссылка, то для безопасности лучше связаться с отправителем по альтернативному каналу связи — телефон или мессенджер

— Привет, это твоё письмо?

Но может быть, что злоумышленник знал, что отправитель собирается послать/послал Вам письмо, и отправитель может дать подтверждение об отправке. Нельзя терять бдительность и изучать письмо далее.

Фишинговые письма, как правило, стараются вызвать ощущения важности и срочности, что бы у жертвы было как можно меньше времени обдумать действия.

*Если пришло уведомление, что в какой-то системе для Вас есть **сообщение или уведомление**, безопаснее авторизоваться привычным образом в этой системе и проверить уведомление.*

Вы решили перейти по ссылке.
Перед этим выполните следующие действия:

→ Внимательно посмотрите адрес ссылки, в ней ничего не должно вызывать подозрение. (наведите мышкой, если это ПК, и в строке уведомлений почтового клиента отобразится адрес ссылки)

→ Скопируйте ссылку и вставьте в систему проверки на вредоносное содержимое virustotal.com, вкладка URL. Эта проверка направлена только на исключение получения вируса по ссылке, угроза фишинга по прежнему актуальна

→ Проверьте, что в начале адреса ссылки «https», а не «http». Этот символ означает защищенное соединение

→ **Перейдите по ссылке.** Если вы провели все предыдущие проверки, то от перехода вреда не будет.

→ Если отобразится **форма авторизации** известного Вам сайта, то нужно сначала на отдельной вкладке браузера по доверенному адресу авторизоваться на этом сайте, затем вернутся и обновить страницу со ссылкой.

→ Если страница обновилась и вы оказались авторизованным на сайте, то все хорошо и ссылка была не фишинговой.

→ Если вы так же увидели страницу авторизации, то с большой вероятностью страница фишинговая и направлена на получения Вашего логина и пароля.

*Чаще всего **фишинговые страницы** похожи на страницы известных банков, но не редко встречаются и по продаже билетов на концерты и массовые мероприятия*

С уважением, команда минцифры
Оренбургской области