В условиях современной цифровой реальности злоумышленники используют все существующие методы обмана для того, чтобы вынудить пользователя совершить действие, которое окажется для него вредоносным, а для мошенников – выгодным.

ПОНЯТИЯ, О КОТОРЫХ НАДО ЗНАТЬ КАЖДОМУ

Социальная инженерия – обман человека с целью побуждения к действиям, выгодным злоумышленнику.

Фишинг (англ. phishing от fishing – рыбная ловля, выуживание) – процесс выманивания конфиденциальной информации. Например, вы вводите пароль от аккаунта в социальной сети на поддельном сайте и нажимаете «Войти» – этот процесс называется фишингом.

Фишинговая ссылка – адрес страницы, на которой злоумышленник крадет конфиденциальную информацию, оставляемую жертвой. Например, ссылка, после перехода по которой у вас просят ввести пароль от почты на поддельном сайте.

Важно! Фишинговые ссылки могут поступать через все каналы: социальные сети, личный и рабочий e-mail, мессенджеры, SMS, а также чаты на сайтах знакомств и подобных ресурсах.

Правило № 1: Лучше не открывать ссылки от незнакомцев.

Правило № 2: Даже ваших знакомых могут взломать, так что, если они вам прислали ссылку без объяснения или с подозрительным объяснением (как если это пишет бот), лучше ее не открывать и проверить, действительно ли это ваш знакомый.

Правило № 3: Если после перехода по подозрительной ссылке у вас запрашивают конфиденциальную или личную информацию, предлагают скачать файл (особенно архив) – уходите с сайта.

Правило № 4: Всегда пользуйтесь современным антивирусом, который может распознать фишинговую ссылку еще «на подлете».

Правило № 5: Проверяйте ссылку не только перед переходом по ней, но и когда вы уже перешли на сайт. Сайт, на который вы попали, может отличаться от того, что было написано в ссылке.

ПРИЗНАКИ ПОТЕНЦИАЛЬНОЙ ОПАСНОСТИ

Ссылка в виде цифр. Пример: http://178.248.232.27.

Ссылка, содержащая символ «@». Настоящий адрес ссылки находится справа от этого символа. Пример: http://bank.ru@zlo.ru.

Ссылки с двумя и более адресами. Пример: https://bank.ru/rd.php?go=https://zlo.ru.

В начале адреса сайта есть www, но нет точки или стоит дефис. Пример: wwwbank.ru или www-bank.ru.

В начале адреса сайта есть http или https, но нет «://». Пример: httpsbank.ru или httpbank.ru.

Если при наведении указателя мыши ссылка выглядит по-другому. Пример: в тексте письма написано tele2.ru, а при наведении мыши в нижнем углу браузера отображается teie2.ru.

Ссылка может быть некликабельна, но содержать подмененные символы. Злоумышленник надеется, что вы скопируете ссылку и вставите в браузер. Пример: в письме указана ссылка tele2.ru, копируете и вставляете в браузер, но оказывается, что это teie2.ru.

Злоумышленник может заменить букву «о» на цифру 0 или маленькую латинскую букву L (l) на большую букву i (I) или b на d и т. д. Пример: 0nline.dank.ru вместо online.bank.ru.

Если ссылка начинается с https:// – это не значит, что она безопасна.

ПРИЗНАКИ ПОДОЗРИТЕЛЬНЫХ СООБЩЕНИЙ, В КОТОРЫХ ВАМ ПРЕДЛАГАЮТ ПЕРЕЙТИ ПО ССЫЛКЕ ИЛИ СКАЧАТЬ ФАЙЛ

Несколько ошибок и описок, отсутствуют пояснения, как если бы это было продолжение разговора (но на самом деле его не велось). Пример: «Здраствуйте, вот обещаная сылка».

Буквы в тексте сообщения частично подменены символами или буквами на другом языке. Пример: «д0брыЙ денb».

Официальные письма с отсутствующими дополнительными контактами (Ф.И.О., должность, телефон, почтовый адрес).

Используется нестандартное оформление официального стиля, который обычно использовался. Пример: без логотипа, другим размером, стилем или цветом шрифта.

ББК 91.9:3

К-16

Составление и оформление Л. А. Гижа

Ответственный за выпуск Т. Д. Шаура

«Как распознать поддельные письма и сайты» : Памятка / МКУК «Куйтунская межпоселенческая районная библиотека им. В.П. Скифа», Сектор информационных и сервисных услуг ; сост. Л. А. Гижа. – Куйтун, 2023. – 4 с. – (Школа цифровых навыков).

Использованы материалы сайта:

«Как распознать фишинговые ссылки и сайты» // РОСКАЧЕСТВО. Портал для умного покупателя : [сайт]. – 2023. – URL: https://rskrf.ru/tips/eksperty-obyasnyayut/fishing/?ysclid=loqn4r8mxn115938952 (дата обращения: 15.11.2023). – Режим доступа: сектор информационных и сервисных услуг.

МКУК «Куйтунская межпоселенческая районная библиотека им. В.П.Скифа»
Сектор информационных и сервисных услуг

Как распознать поддельные письма и сайты

Школа цифровых навыков

Памятка

12+

Куйтун 2023

Куйтун, 2023