Криминальное искушение социальной инженерии

Высота и агрессивность шквалов кибератак в последнее время не снижается. Нередко они совершаются с помощью приемов социальной инженерии, то есть манипуляций действиями человека практически без применения технических средств...

Об этой и иных тенденциях в сфере кибербезопасности рассказал **Михаил ПРИБОЧИЙ,** управляющий директор «Лаборатории Касперского» в России, странах СНГ и Балтии, выступая на международном форуме #GBC (Государство. Бизнес. Граждане).

– Методы социальной инженерии активно используются и в спамерских звонках, которые сегодня являются распространенной напастью в СНГ. В целом вероятность, что звонок с неизвестного номера окажется спамерским, составляет 60–80 %, и около 6 % из них скорее всего окажутся мошенническими. А недавний опрос, который мы проводили в Беларуси, показал, что в 2020 году с телефонным мошенничеством не понаслышке знаком почти каждый третий (31 %).

Злоумышленники часто делают ставку на человеческий фактор, например, стараются напугать либо вызвать любопытство того, кому звонят. Очень часто они представляются сотрудниками банков или государственных учреждений. Такой подход, к сожалению, оказывается весьма действенным. Человека проще убедить распрощаться со своими деньгами, если он думает, что общается с сотрудником солидной организации. Поэтому категорически не стоит сообщать третьим лицам конфиденциальную информацию, кем бы они ни представлялись. Также не стоит скачивать какие-либо программы по их просьбе или переходить по ссылкам, которые они присылают. Настоящие сотрудники банков никогда не будут запрашивать одноразовые коды из СМС или персональные данные по телефону, тем более не будут просить перейти по ссылке или скачать тот или иной софт.

Мошенники не только звонят, но и активно ищут жертв в интернете, например, расставляют ловушки в виде скама. Скам – это мошеннические рассылки и объявления, обещающие пользователям крупное денежное поступление. В частности, в мае этого года эксперты «Лаборатории Касперского» зафиксировали в Беларуси фейковую рассылку от Министерства здравоохранения, в которой обещали материальную помощь в связи с коронавирусной инфекцией в размере от 250 до 750 белорусских рублей. Для придания достоверности в объявлении указывалось, что сумма выплаты зависит от профессии получателя – якобы работникам медицинских учреждений, спасателям и государственным работникам полагаются более крупные выплаты.

Всего за первые шесть месяцев 2021 года «Лаборатория

Касперского» предотвратила почти 1,5 миллиона попыток перехода белорусских пользователей на фишинговые страницы. Из них более 470 тысяч – на скам-ресурсы. При этом доля спама в почтовом трафике Беларуси в первые шесть месяцев 2021 года, по данным компании», составила 42,55 %.

Зачастую злоумышленникам даже не приходится применять сложные тактики, чтобы выудить личную информацию или данные, которые позволят получить доступ к аккаунту, в том числе банковскому, ведь меры безопасности соблюдают далеко не все. Так, 60 % белорусских пользователей, согласно нашему опросу, предпочитают регистрироваться на сайтах или в сервисах с помощью аккаунта в социальной сети, а не создают новую учетную запись. Проблема в том, что если злоумышленник получит доступ к аккаунту в социальной сети, он легко сможет проникнуть и в другие учетные записи. Почти каждый второй (46 %) использует одинаковый пароль либо пароль, который отличается на один-два символа, для всех личных аккаунтов, а ведь создание сложных и разных паролей – это один из ключевых способов защитить свои устройства и данные от утечек и взломов.

Еще одна актуальная сегодня тема – это детская онлайн-безопасность. По данным опроса «Лаборатории Касперского», 60 % родителей в Беларуси непосредственно сталкивались с киберугрозами в отношении детей. Так, 43 % респондентов отметили, что их дети получали предложения дружить от людей, которых не знали, в 39 % случаев это были незнакомые взрослые. Кроме того, дети склонны к чрезмерной открытости в интернете: 42 % указывают в общедоступном профиле свой настоящий возраст, 26 % – номер школы, 10 % делятся именами и фамилиями родителей или родственников, еще 10 % – фотографиями, где видно обстановку квартиры. Казалось бы, сама по себе публикация таких данных не несет никакой угрозы, но злоумышленники могут собирать их и использовать в своих целях, чтобы выследить ребенка или заставить его перевести деньги с родительских карт, ведь они понимают, что втереться в доверие легче, если знаешь, например, имена родителей или номер школы. Становится все более распространенным такое явление, как овершеринг – публикация излишней информации о себе в интернете.

Все это говорит о том, что вопрос повышения уровня цифровой грамотности стоит очень остро. Взрослым нужно знать, какие бывают риски и схемы мошенничества в интернете, чтобы понимать, чего стоит избегать и о чем нужно предупредить детей. Важно регулярно проговаривать базовые правила безопасного поведения в онлайне и социальных сетях и вообще больше говорить с детьми на разные темы, чтобы они не боялись задавать вопросы и знали, что родители придут на помощь в случае столкновения с чем-то непонятным, неприятным или даже стыдным.

Социальные сети – одна из самых популярных категорий сайтов для детей. Но не всегда взрослые уделяют достаточно внимания этой стороне онлайн-жизни детей. В частности, 39 % родителей не заходят на страницу своего ребенка, а 28 % не находятся друг у друга в друзьях. Мы напоминаем: стоит знать, что ребенок делает в интернете, но, конечно, лучше, если взрослый искренне этим интересуется. Контроль не должен превращаться в слежку, не надо пытаться угнаться за всеми перемещениями и переписками ребенка, но стоит знать, с кем он общается и какие у него увлечения в сети.

В помощь родителям существуют специальные решения. Например, есть программа Kaspersky Safe Kids, которая совместима со всеми популярными платформами: Windows, macOS, Android и iOS. Она позволяет быть в курсе, сколько времени ребенок проводит в интернете, какие сайты посещает, а также умеет определять текущее местоположение благодаря функции геолокации. Последнее может быть удобно, если ребенку приходится возвращаться домой из школы или секций одному. Не так давно в решении появилась функция «Безопасный поиск на YouTube», которая дополняет штатные возможности популярного видеохостинга, позволяя исключить доступ к сомнительному контенту, в котором присутствуют, скажем, алкоголь, табакокурение или ненормативная лексика.

Самая действенная стратегия для защиты от киберугроз сегодня – сочетать технические и нетехнические меры. Надежное защитное решение, которое умеет блокировать не только вредоносные, но и потенциально опасные программы, а также фишинговые ресурсы, – это эффективная и важная мера, но необходимо уделять должное внимание в том числе настройкам приватности, своевременно обновлять ПО и скачивать приложения только из официальных магазинов.

Вдобавок к установке защитных решений, доказавших свою эффективность, следует постоянно повышать уровень цифровой грамотности: свой собственный, своих детей и пожилых родственников, а для предпринимателей – еще и сотрудников их компаний.