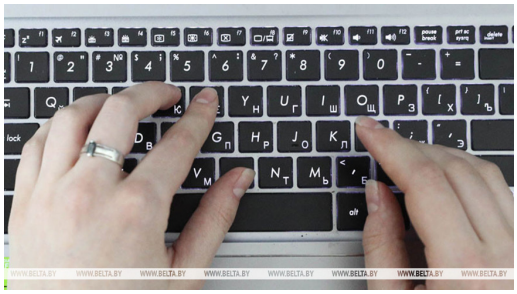
Встретили фишинговый сайт. Куда обратиться, рассказали в Центре защиты персональных данных

Автор: Администрация
11.04.2024 05:29 -



Куда обращаться, если встретился фишинговый сайт, как обезопасить себя от мошенников и как происходит закрытие доступа к фальшивым сайтам, если он находится в зарубежной доменной зоне, рассказала корреспонденту БЕЛТА заместитель начальника управления образовательных услуг и связей с общественностью Национального центра защиты персональных данных Ольга Шибко. Специалист рассказала, куда может обратиться обычный человек, если встречает фишинговый сайт. “В случае обнаружения вредоносного программного обеспечения или подозрительного интернет-ресурса, который находится в национальном сегменте сети интернет, необходимо обратиться в Национальный центр реагирования на компьютерные инциденты Республики Беларусь (CERT.BY)”, – отметила она. Сделать это можно, направив письмо на адрес support@cert.by с темой “СПАМ”. Также обратиться можно через форму “Сообщить об инциденте” на сайте CERT.BY. Он осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории Беларуси. “Если же вы стали жертвой кибермошенников, необходимо оперативно обращаться в правоохранительные органы”, – подчеркнула заместитель начальника. Рассказала она и о мерах безопасности в интернете. “Каждый может принять ряд мер для защиты от фишинговых ресурсов. Так, при получении подозрительных сообщений или переходе по ссылкам будьте бдительны. Обращайте внимание на грамматические ошибки, искаженные, не соответствующие действительности наименования доменов или необоснованные запросы личной информации. Перед вводом личных данных убедитесь, что сайт использует защищенное соединение (HTTPS). Обратите внимание на замок в адресной строке браузера”, – поделилась Ольга Шибко. Посоветовала заместитель начальника и использовать лицензионное антивирусное программное обеспечение. А также не открывать подозрительные ссылки из писем, особенно если они пришли от неизвестных отправителей и если они касаются любых финансовых операций, выплат, выигрышей и т.д. “Некоторые фишинговые атаки могут приходить через вредоносные вложения в письмах. Не скачивайте и не открывайте файлы, если вы не уверены в их подлинности и (или) не уверены в надежности отправителя”, – отметила она. Еще одна мера предосторожности, это не оставлять свои персональные данные на ненадежных сайтах. “Если у вас есть сомнения относительно подлинности сайта или сообщения, свяжитесь с организацией напрямую через официальные контакты”, – посоветовала Ольга Шибко. По ее словам, в последние годы наблюдается устойчивая тенденция к

росту использования мошенниками фишинговых сайтов. Киберпреступники непрерывно работают, разрабатывая новые и все более изощренные методы обмана. “Фальшивые сайты могут имитировать популярные онлайн-платформы, банки, социальные сети или сервисы электронной почты. Их внешний вид, функциональность могут быть практически неотличимы от настоящих”, – подчеркнула заместитель начальника. “Появились новые способы использования нейросетей. Так сегодня искусственный интеллект позволяет несложным путем создавать вредоносные программы или писать фишинговые письма для эффективного распространения троянов. То есть код можно написать без навыков программирования, а фишинговое письмо сделать персонализированным, убедительным и на любом иностранном языке. Это очень опасно для доверчивых пользователей”, – добавила Ольга Шибко. Центром на регулярной основе проводится мониторинг сети интернет на предмет нарушений законодательства о персональных данных. При этом чаще всего нарушения касаются незаконного сбора или распространения персональных данных без использования фишинговых сайтов. НЦЗПД постоянно принимаются меры для безопасности интернет-пространства. Так, недавно сотрудники центра закрыли доступ к фальшивому сайту Министерства труда и социальной защиты, через который мошенники пытались получить доступ к счетам белорусов. Сайт был расположен в зарубежной доменной зоне. “В случае обнаружения интернет ресурса в зарубежной доменной зоне, где были распространены персональные данные белорусов, или же фишинговых сайтов, собирающих личные и финансовые данные граждан Беларуси, Национальный центр защиты персональных данных взаимодействует с уполномоченным органом по защите прав субъектов персональных данных иностранного государства, обращается к зарубежным регистраторам доменных имен (которые зарегистрировали фишинговый домен), собственникам интернет-ресурсов”, – поделилась Ольга Шибко.

Источник