Компрометация корпоративной электронной почты

Предупреждение о безопасности поставщиков.

Компания MSD серьезно относится к случаям мошенничества и заботится об информационной безопасности.

Вам следует знать о том, что в связи с массовым переходом на виртуальные способы коммуникации случаи компрометации корпоративной электронной почты (BEC-аферы) участились. При BEC-аферах мошенник использует электронную почту или иные средства виртуальной коммуникации, чтобы выдавать себя за руководителя, сотрудника или иное уполномоченное лицо.
Затем мошенник от лица представителя компании просит выплатить ему средства или предоставить доступ к информации о зарплате сотрудников или об удержанных с них налогах.

Что вам следует знать

Задача MSD — защитить вашу деловую и банковскую информацию. В соответствии с указаниями нашего Глобального отдела по вопросам соблюдения конфиденциальности, нашими технологическими процессами и рекомендациями, а также местными и региональными правилами специально обученный персонал нашей компании при сборе, проверке и сохранении данных строго соблюдает утвержденные процессы и методы контроля. У нас существует ряд точек контроля, а наши процедуры и принятые практики регулярно подвергаются аудиту.

Чтобы лучше защитить ваш бизнес:

- Используйте дополнительные каналы и двухфакторную проверку подлинности для независимой проверки запросов на изменение информации, содержащейся в учетной записи.
- Проверяйте соответствие URL-адресов, содержащихся в переписке, предприятиям, работниками которых представляются ваши собеседники.
- Обращайте внимание на гиперссылки, в которых доменное имя указано с ошибкой.
- Проверяйте соответствие адреса электронной почты, с которого вам присылают сообщения, отправителю, особенно в случаях, когда вы проверяете почту с мобильного устройства.
- Установите фильтры системы обнаружения атак, чтобы помечать сообщения с адресов, напоминающих корпоративные. Например, если правильный адрес выглядит как ceo@abc_company.com, то письма с адреса ceo@abc-company.com будут помечаться как подозрительные.
- Регулярно проверяйте финансовые счета на предмет несоответствий, например отсутствия средств.
- Регулярно устанавливайте исправления и обновляйте программное обеспечение во всех системах.

- Отрегулируйте настройки на рабочих компьютерах так, чтобы электронные адреса были видны полностью.
- Узнайте контактную информацию вашего местного центра устранения проблем и информируйте центр о ваших подозрениях в части BEC-афер в отношении MSD. Также вы можете обратиться в местные правоохранительные органы.

Нас называют MSD везде, кроме США и Канады, где мы известны как Merck & Co Inc, Rahway, NJ, США.