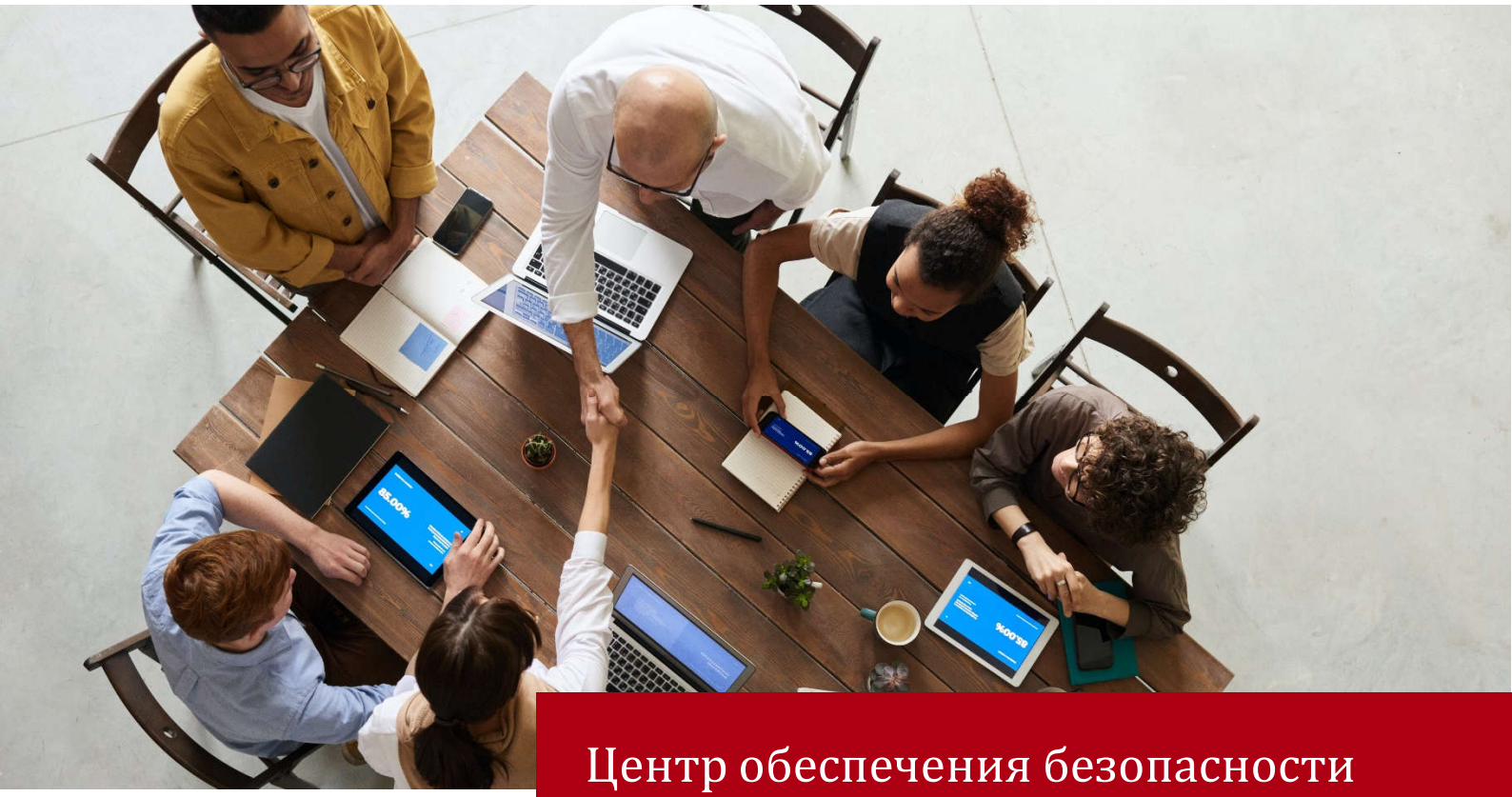
ThreatMark

SBERBANK



Центр обеспечения безопасности ThreatMark помогает Сбербанку противостоять интернет-мошенничеству и оптимизировать антимошеннические процессы

ThreatMark помогает банку создать защищенную от угроз систему интернет-банкинга с привлечением специально выделенной команды сотрудников нашего Центра обеспечения безопасности. Инженеры нашей компании непрерывно анализируют и выявляют новые фишинговые веб-сайты и вредоносное программное обеспечение. Они оказывают оперативную помощь в решении конкретных проблем и предоставляют консультативную поддержку для улучшения антимошеннических систем наших клиентов. В частности, команда ThreatMark тесно сотрудничает с сотрудниками Сбербанка, чтобы общими усилиями противостоять мошенникам и защитить клиентов банка.

Сбербанк— крупнейший российский банк, который насчитывает 20 000 отделений и свыше 260 000 сотрудников по всему миру. В России 70 % населения пользуются услугами 11 территориальных банков и 14 000 отделений. Международная сеть банка состоит из дочерних организаций, отделений и представительств, расположенных в 21 стране мира, в том числе в Чехии.

Сотрудничество между двумя компаниями началось в 2017 году. В то время Сбербанк искал инновативное решение для того, чтобы повысить уровень безопасности своих физических и юридических лиц. Основной проблемой было осуществление несанкционированных и мошеннических транзакций, и банк искал возможности защитить своих клиентов и повысить их уровень доверия. В результате банк принял решение воспользоваться услугами Центра обеспечения безопасности ThreatMark и внедрить антимошенническое решение, разработанное компанией.

О Центре обеспечения безопасности

Центр обеспечения безопасности — один из важнейших компонентов, которым пользуется большинство клиентов ThreatMark. Он позволяет получать преимущества упреждающего выявления и анализа киберугроз и вредоносных программ.

«Мы ценим, что ваша команда по борьбе с интернет-мошенничеством дает нам возможность отслеживать действия злоумышленников и сообщать нашим инженерам о появлении новых киберугроз в цифровом пространстве».

Клара Виткова (Klára Vítková), старший специалист группы противодействия мошенничеству
Сбербанк в Чехии

Команда Центра обеспечения безопасности ThreatMark использует в своей работе два уникальных источника для анализа - элементы на странице и внешние элементы. Элементы на странице включают в себя обезличенные данные, полученные от банков-клиентов ThreatMark, такие как неизвестные примеры вредоносных кодов, фишинговые атаки, подозрительные операции, идентификаторы устройств и модели поведения пользователей. К внешним элементам относятся различные собственные методы сканирования и изучения интернет-пространства, позволяющие выявлять новые угрозы и активность вредоносных программ. Полученная из обоих источников информация объединяется и тщательно анализируется.

На основе аналитической работы создаются сигнатуры — описания отличительных признаков вредоносных программ. После проведения начальной аналитической обработки сигнатуры передаются в единый Центр безопасности и автоматически добавляются в черные списки у всех клиентов. Важно отметить, что ThreatMark способен обнаружить не только известные вирусы, но и те, которые еще ранее не выявлялись (т.н атаки нулевого дня). Объединяя данные, собранные в веб - и мобильных приложениях банка и данные, полученные из других источников, ThreatMark всесторонне их анализирует, что позволяет компании оперативно обнаруживать и устранять все киберугрозы.

Проведение консультаций и семинаров

Сотрудники Центра обеспечения безопасности ThreatMark также ведут консультативную и образовательную деятельность для наших клиентов. По запросу банка наша команда может организовать и провести семинар по новейшим киберугрозам и способам их предотвращения. Для представителей Сбербанка был проведен

двухдневный семинар, посвященный новым видам банковских вирусов. В ходе мероприятия были приведены реальные примеры угроз и рекомендации по их выявлению и устранению.

Отзывы, которые сотрудники ThreatMark получили от Сбербанка, подтверждают необходимость своевременной организации образовательных мероприятий и инструктажа по повышению осведомленности в вопросах безопасности.

Из высказывания Клары Витковой: *«В течение трехлетнего сотрудничества Сбербанка и ThreatMark мы высоко оценили, что ваша команда по борьбе с интернет-мошенничеством дает нам возможность отслеживать действия злоумышленников и сообщать нашим инженерам о появлении новых киберугроз в цифровом пространстве. Мы считаем, что в команде ThreatMark работают исключительно профессионалы своего дела, и Сбербанк высоко ценит совместную работу с ними».*

Заключение

Оптимальный способ защиты любой системы в Интернете предусматривает использование технических и человеческих факторов. Подобно тому, как злоумышленники применяют высокие технологии, чтобы обмануть людей, так и эффективное решение должно сочетать в себе оба фактора. Такой комплексный подход используется в ThreatMark AFS, модульном полнофункциональном решении по предотвращению банковского мошенничества. Оно позволяет обнаружить киберугрозы, подтвердить личность пользователей посредством поведенческой биометрии и выявить мошенничество с платежами в реальном времени благодаря использованию алгоритмов машинного обучения и бизнес-правил. Как в случае со Сбербанком,

Центр обеспечения безопасности компании ThreatMark помогает предотвращать угрозы с помощью многоканальных методов сбора данных. Помимо использования высоких технологий команда Центра работает над устранением рисков и угроз, задействуя человеческий фактор, предоставляя персоналу банка все необходимое для защиты клиентов и их обучения.

ThreatMark s.r.o.

Hlinky 505/118,
603 00 Brno,
Чешская Республика

ИН: 04222091, ИНН: CZ04222091

Обратная связь:
info@threatmark.com