

Полная защита от фишинга на мобильных устройствах

100-процентная адаптация пользователя

Ключевые преимущества

- 100-процентная адаптация пользователя
- Комплексная защита от фишинга и его устранение
- Контроль баланса между безопасностью и конфиденциальностью

Обзор

С помощью фишинговых атак злоумышленники обманом вынуждают пользователей делиться персональными данными, которые могут быть использованы для мошенничества. Например, пользователь может кликнуть на ссылку, отправленную злоумышленником, и предоставить ему свои учетные данные. Пользователя также могут убедить скачать на свое устройство

ivanti.com



вредоносное ПО или набор эксплойтов. Согласно отчету Data Breach Investigations Report (DBIR) 2021 года компании Verizon, фишинг-атаки третий год подряд являются главной причиной утечки данных. Популярность этого вида атак постоянно растет. С 2019 по 2020 год процент случаев утечки данных, в которых были задействованы фишинговые атаки, вырос на 25%.¹



Почему взломщики все чаще атакуют мобильные устройства?

На это есть ряд причин. Сегодня в компаниях количество мобильных устройств намного превышает количество привычных конечных точек (ПК и ноутбуки). Несмотря на это, многие организации не уделяют должного внимания безопасности мобильных устройств. Так часто происходит потому, что эти компании еще не столкнулись с утечкой данных или просто не подозревают о такой угрозе. В результате на защиту мобильных устройств тратится мизерная

часть бюджета, выделяемого на безопасность конечных точек. Кроме того, мобильные устройства являются привлекательной целью для злоумышленников из-за своих маленьких экранов, на которых пользователям сложно рассмотреть важную информацию и принять взвешенное решение. Стоит также отметить, что подлинность сообщений бывает сложно подтвердить.

Комплексная защита от фишинга с Ivanti Mobile Threat Defense (MTD)

Ivanti Mobile Threat Defense (MTD) предоставляет защиту от фишинга на устройствах и в облаке. Так MTD обеспечивает безопасность интернет-трафика на всех устройствах iOS и Android в рабочем пространстве, где корпоративные данные свободно перемещаются между устройствами и облачными серверами, обеспечивая продуктивность вне зависимости от места работы. Активация MTD на мобильных устройствах, управляемых с помощью Ivanti UEM, не требует никаких действий со стороны пользователя. Ей удаленно управляют администраторы.

100-процентная адаптация пользователя

MTD легко внедряется и обеспечивает защиту и устранение атак, происходящих на уровне устройств, сетей и приложений. Для активации MTD не требуется никаких действий со стороны пользователя, что позволяет добиться 100-процентной адаптации. Соответствие требованиям на всех уровнях поможет поддерживать адаптацию и повысить общий уровень защиты компании.

Комплексная защита от фишинга и его устранение

MTD выявляет и устраняет фишинговые атаки по всем направлениям, включая не только корпоративную электронную почту, но и SMS сообщения, социальные сети и другие способы коммуникации. Комплексная защита от фишинга использует машинное обучение на устройстве и поиск по базам данных. Подключите облачный поиск фишинговых URL-адресов для повышения эффективности обнаружения. Также с помощью аналитики фишинга можно понять, насколько хорошо ваша компания от него защищена.

Контроль баланса между безопасностью и конфиденциальностью

MTD позволяет компаниям контролировать баланс между безопасностью и конфиденциальностью данных пользователей, в зависимости от их нужд и комфорта. Используйте эффективное обнаружение фишинга только на устройствах или добавьте обнаружение в облаке. Выбор за вами!

Полная защита от фишинга на мобильных устройствах

MTD предоставляет защиту от фишинга на устройствах и в облаке, обеспечивая безопасность интернет-трафика на всех устройствах iOS и Android в рабочем пространстве. Активация MTD на мобильных устройствах, управляемых с помощью Ivanti UEM, не требует никаких действий со стороны пользователя. Ей удаленно управляют администраторы, что позволяет достичь 100-процентной адаптации пользователей без снижения продуктивности. Чтобы повысить безопасность рабочего пространства и снизить риск фишинговых атак, компании могут внедрить решение Ivanti Zero Sign-On (ZSO) которое обеспечивает безопасную беспарольную аутентификацию в облачные сервисы компании.



ivanti



[ivanti.com](https://www.ivanti.com)

1 800 982 2130

sales@ivanti.com

1. Verizon: 2021 Data Breach Investigations Report.
<https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/>