ФИШИНГ — ДЕЛО СЕРЬЕЗНОЕ

Известно, что фишинг является одним из главных источников доходов для хакеров. Поэтому фишинговые атаки представляют для организаций серьезную угрозу финансовой безопасности.

Одно из последних исследований показывает, насколько сильно возросла данная угроза: Средняя компания со штатом в 10 000 сотрудников тратит 3,7 миллионов долларов США в год на устранение последствий фишинговых атак. Средний работник в год тратит около 4,16 часов на фишинговые сообщения.

Основная доля издержек, которые организации несут вследствие фишинговых атак, приходится на следующие области: хищение баз данных по взломанным учетным записям и вредоносные программы, а также расходы на локализацию вредоносных программ до их распространения на всю сеть.

Способны ли ваши работники эффективно противостоять данной угрозе или они уязвимы перед Интернет-мошенниками?

“Средний работник в год тратит около 4,16 часов на фишинговые сообщения.”

ПОЧЕМУ ИНФОРМИРОВАННОСТЬ О ФИШИНГЕ НЕ ЗАЩИТИТ ВАС ОТ МОШЕННИКОВ

Как специалисты по безопасности мы доверяем проверенным методам, а не субъективным мнениям.

Поэтому мы знаем, что простая информированность о существовании проблемы не решает ее. Вы должны быть готовы решать данную проблему на практике.

Другими словами, информированность — это бездействие.

С точки зрения корпоративной безопасности, при любом сценарии риска «боеготовность» эффективнее информированности. Например, работники, открывающие с виду безобидное приложение к электронному письму, могут не распознать тщательно завуалированные хакером признаки мошенничества, даже если они знают о существовании фишинга.

В большинстве обучающих программ сделан акцент на информировании работников о фишинге, и по этим же критериям проводится оценка их знаний. Мы в CybeReady считаем, что это только половина успеха.

Если вам угрожает фишинг, важно принять меры, которые позволят снизить риск того, что ваши работники станут жертвой атаки.

НЕ СЛЕДУЕТ НЕДООЦЕНИВАТЬ СТОИМОСТЬ И СЛОЖНОСТЬ КОРПОРАТИВНОГО ОБУЧЕНИЯ

При покупке обучающих материалов и технологий большинство организаций принимает в расчет только стоимость начальных вложений. Исключительный акцент на материальных затратах дает вам неполную картину, снижая эффективность инвестиций. Реальные вложения начинаются уже после внедрения программы.

После оценки стоимости программ обучения безопасности, критически важно учесть три аспекта: стоимость подготовки к обучению, временные затраты на обучение работников и стоимость вовлеченности.

РАЗБЕРЕМ ДАННЫЕ РАСХОДЫ В ОТДЕЛЬНОСТИ.

СТОИМОСТЬ ВОВЛЕЧЕННОСТИ:

Это нематериальные расходы, характерные для любой обучающей программы. Заботятся ли ваши работники о безопасности? Считают ли они вашу программу пустой тратой времени? Хорошая обучающая программа всегда повышает вовлеченность работников, а плохая — отталкивает.

ВРЕМЕННЫЕ ЗАТРАТЫ НА ОБУЧЕНИЕ РАБОТНИКОВ:

Эти косвенные издержки включают время, затраченное на обучение, и соответствующее рабочее время. (Под рабочим временем понимается время, которые требуется для того, чтобы собрать всех работников для обучения, будь то собрание в конференц-зале или удаленное устранение технических неисправностей.)

СТОИМОСТЬ ПОДГОТОВКИ К ОБУЧЕНИЮ:

Данные прямые расходы включают оплату услуг третьих лиц (консультанты, лицензии на программное обеспечение), а также временные издержки, связанные с управлением программой, мониторингом работы обучающего программного обеспечения и настройкой системы.

Ведущие мировые организации из различных областей, от здравоохранения и страхования до банковского сектора, доверяют CybeReady подготовку своих сотрудников для противодействия фишингу.

CybeReady предлагает программы Phishing Readiness, которые полностью адаптированы к особенностям вашего региона, отрасли и бренда.

АНАЛИТИЧЕСКИЙ ОТЧЕТ READINESS

Узнайте свои слабые места.Чрезвычайно важно видеть полную картину: почему ваши работники попадаются на уловки мошенников, какие отделы наиболее уязвимы и другие факторы риска. CybeReady позволяет вам принимать обоснованные решения на базе комплексного анализа и отслеживать эффективность с течением времени.

НЕПРЕРЫВНОЕ ОБСЛУЖИВАНИЕ

Мы предоставляем комплексное решение. С нашей программой Readiness, разработанной и внедряемой профессионалами своего дела, вы будете во всеоружии. Это решение позволит вам осуществлять мониторинг устойчивости вашей организации к фишинговым атакам и эффективно обучать персонал инструментам их предотвращения, а также находить выход из нештатных ситуаций, которые могут ввести ваших работников заблуждение.

ИМИТАЦИОННЫЕ АТАКИ

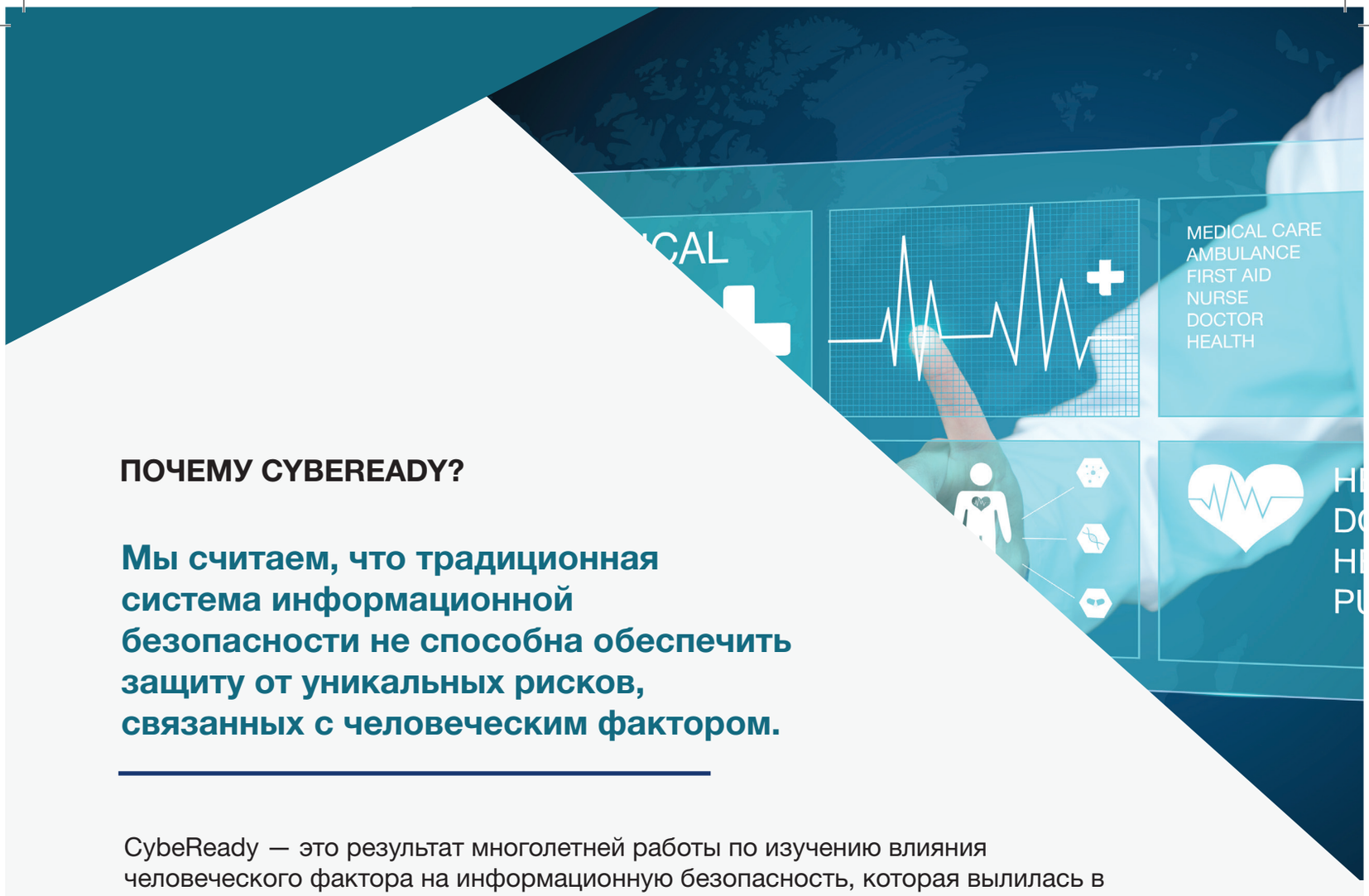
Наш тренинг имитирует реальность.Программа CybeReady имитирует не какую-то одну отдельно взятую ситуацию, а воспроизводит целую серию атак в контексте как внешних событий (праздники, конференции), так и внутренних событий (обновления программного обеспечения, пенсионные программы). Таким образом, вы сможете подготовить ваших работников к различным видам фишинговых атак.

НЕ ТРЕБУЕТСЯ УСТАНОВКА

Мы берем на себя организационные вопросы. Благодаря облачной технологии CybeReady вам не нужно устанавливать программное обеспечение, приобретать новое оборудование и проводить техническое обслуживание. Никакой головной боли и подводных камней: всего 48 часов и вы сможете пользоваться отлаженной системой, работу которой обеспечивают профессионалы.

ПОЛНОСТЬЮ АДАПТИРОВАННЫЙ КОНТЕНТ

Мы считаем, что шаблоны для роботов. Только поведенческий тренинг может обеспечить защищенность ваших работников от мошенников. CybeReady создает реалистичные фишинговые атаки различного уровня сложности, от уникальных характерных для конкретной отрасли сообщений до сообщений, ориентированных на тот или иной отдел или должность. Весь контент соответствует вашему виду деятельности и адаптирован с языковой и культурной точки зрения.



ПОЧЕМУ CYBEREADY?

Мы считаем, что традиционная система информационной безопасности не способна обеспечить защиту от уникальных рисков, связанных с человеческим фактором.

CybeReady — это результат многолетней работы по изучению влияния человеческого фактора на информационную безопасность, которая вылилась в создание новой концепции, получившей название Employee Cyber Readiness.

Благодаря глубокому пониманию процессов и решений, связанных с управлением человеческих рисков, компания создала высокоэффективную антифишинговую программу. CybeReady специализируется на специфических рисках информационной безопасности, источником которых является работник, которые редко (если вообще) учитываются в программах обучения.

В ответ на эту проблему CybeReady создала свое антифишинговое решение, суть которого точно описывает знаменитая фраза из Шекспира:

«БЫТЬ ГОТОВЫМ — ВОТ ВСЕ».

THE HUMAN READINESS COMPANY
CYBEREADY

info@cybeready.com | www.cybeready.com