Формирование и повышение культуры кибербезопасности.

Опыт Сбербанка

Ксения Лопатина, *начальник отдела киберкультуры Сбербанка, кандидат философских наук*

Сегодня крупнейшие цифровые компании вносят свой вклад в формирование культуры кибербезопасности, интегрируя ее в корпоративную. Год от года наблюдается рост киберпреступности. Мошенники ищут “слабое звено” в компании, через которое могут получить доступ к ее системам, и чаще всего таким звеном оказывается человек. Начальник отдела киберкультуры Сбербанка Ксения Лопатина в своем интервью поделилась опытом, какие меры предпринимает Сбербанк по повышению киберграмотности не только сотрудников, но и клиентов.

1841 год

дата основания банка

70%

населения России пользуются услугами Сбербанка

14 275

подразделений в 83 субъектах Федерации*

** данные на 01.01.2019*

– Какое определение вы даете понятию "культура кибербезопасности"?

– Мы отталкиваемся от определений кибербезопасности и культуры, которая выступает предметом изучения множества наук. Из огромного количества существующих определений культуры мне нравятся два. Одно из самых распространенных – культура как человеческая деятельность в ее самых разных проявлениях, включая накопление человеком и социумом в целом навыков и умений. Второе – культура как набор правил, которые предписывают человеку определенное поведение с присущими ему переживаниями и мыслями и оказывает на него тем самым управленческое воздействие. Если объединить их с определением кибербезопасности как реализации мер по защите систем, сетей и программных приложений от цифровых атак, получаем следующее: культура кибербезопасности – навыки, умения и набор правил, которыми руководствуется человек с целью защиты от цифровых атак различных аспектов своей деятельности.

– Почему необходимо формировать именно культуру кибербезопасности, а не, скажем, повышение осведомленности?

– Повышение осведомленности – это информирование, передача и формирование знаний. И наши усилия в том числе в первую очередь направлены на формирование знаний в сфере кибербезопасности. Но очень часто мы сталкиваемся с ситуациями, когда человек знает, но не применяет или, что еще хуже, сознательно старается обойти правила. Именно поэтому наша цель – достичь такого поведения пользователей, при котором они будут следовать основным правилам кибербезопасности в своей деятельности на уровне привычки. Поэтому мы используем понятие "культура кибербезопасности".

Привить стойкие знания человеку, сформировать правила, которым он будет следовать в своей повседневной жизни, можно только при следующих условиях: человек понимает, для чего ему эти знания необходимы, общество разделяет с ним ценность этих знаний, следование тем или иным правилам типично для среды, в которой человек оказался.

– Какие элементы включает культура кибербезопасности? В чем важность каждого из них?

– Таких элементов много, и их совокупность формирует почву, на основе которой создаются знания. Основные элементы культуры – традиции, ценности, язык, символы, правила. Их необходимо формировать одновременно с созданием знаний в сфере кибербезопасности. Такой подход позволяет сделать мероприятия, направленные на распространение этих знаний, максимально эффективными.

Традиции, основа любой культуры, – элементы социального и культурного наследия, которые сохраняются в том или ином сообществе, являются необходимым условием его жизнедеятельности и передаются из поколения в поколение. Прочесть раз в неделю информационный дайджест по кибербезопасности, погрузиться в информационное поле ежеквартальной газеты Cyber life, проанализировать проблемы и достижения на ежегодной сессии кибербезопасности – это новые традиции, которые появились в нашей Службе кибербезопасности. Они объединяют сотрудников и мотивируют к развитию знаний.

Ценности – это социально значимые предпочтения, сегодня они в том числе мотивируют повышать свою кибер-

KASPERSKY lab

Кибербезопасность крупных организаций и предприятий

Комплексная платформа для защиты крупных IT-инфраструктур и промышленных сред

www.kaspersky.ru/enterprise

#ИстиннаяБезопасность

Главная цель стратегии 2020

Реализация инициатив, которые позволят Банку выйти на новый уровень конкурентоспособности, дающий возможность конкурировать с глобальными технологическими компаниями, оставаясь лучшим банком для населения и бизнеса.

В сегодняшнем Сбербанке почти ничего не напоминает о сберегательных кассах, функции которых он выполнял на протяжении значительного периода своей истории. Сбербанк не только шагает в ногу с современными тенденциями рынка, но и опережает их, уверенно ориентируясь в стремительно меняющихся технологиях и предпочтениях клиентов.

грамотность. Что касается правил, то они регулируют поведение в соответствии с ценностями. Безопасность – общекультурная ценность, которая детализируется в профессионализме, саморазвитии, следовании правилам кибербезопасности (разумеется, включая правила своей организации) и обучении этим правилам других.

Ценности в области кибербезопасности формируются в том числе благодаря просветительской работе: статьям и докладам сотрудников служб кибербезопасности, вовлечению в проблематику кибербезопасности путем геймификации.

Язык – знаковая система, которая используется в конкретном социуме и выполняет функции создания, хранения и передачи информации. Несмотря на развитие технологий, проблема коммуникаций не теряет своей актуальности, что порождает проблемы в том числе в области кибербезопасности: инциденты зачастую происходят из-за того, что специалистам не удалось понять друг друга.

Компании имеет смысл создать для сотрудников единую точку входа, куда можно обратиться по любому вопросу кибербезопасности и получить компетентный оперативный ответ. Самый очевидный вариант – "живой" ящик. Возможно и более продвинутое решение: например, мы в этом году создали центр поддержки кибербезопасности. Это горячая линия, по которой любой сотрудник, с одной стороны, может решить свою проблему и защитить себя, а с другой – помочь службе кибербезопасности предотвратить инцидент на стадии его зарождения и тем самым защитить банк.

Символика тоже очень важна. Мы проводим мероприятия по формированию культуры кибербезопасности уже третий год, и все это время развивается наш бренд SCS – Sberbank Cyber Security. Имеет смысл напомнить, что знаки различия относятся к числу древнейших артефактов: еще в древности особые символы позволяли отличить членов одного рода от другого. Такие знаки испокон веков поддерживали и объединяли людей. Сегодня логотип SCS объединяет нашу службу кибербезопасности. Его использование в коммуникациях указывает на высокий контроль качества, а использование брендированной продукции – на принадлежность к команде.

Когда создается единое поле коммуникации, а сотрудники чувствуют себя частью команды, которая разделяет общие традиции и ценности, возникает основа для повышения осведомленности, непрерывного обучения сотрудников и клиентов.

– Если говорить о начале и середине нулевых годов, то как в это время учили безопасности? Ведь в начале все работы в области ИБ были некой принудительной "обязаловкой"? Изменилась ли ситуация с развитием технологий?

– В начале нулевых годов в принципе и учили, и учились иначе. Развитие технологий изменило образ жизни и, с одной стороны, сформировало новые особенности обучаемых, которые необходимо учитывать при выборе методов обучения, а с другой – обеспечило нас новыми технологичными эффективными методами обучения.

Мы проанализировали наиболее распространенные способы обучения и особенности современного обучаемого. Он просматривает текст, а не читает его слово за словом, готов неформально обучать других. Этот человек достает и просматривает смартфон девять раз в час, 27 раз в день использует сервисы и приложения, работающие через Интернет. Современный обучаемый доступен не более пяти секунд, чтобы привлечь внимание, не заинтересован смотреть обучающее видео длиннее четырех минут, требователен к формату подачи материала. Он привык получать информацию по точечному запросу и в 60 раз быстрее обрабатывает изображение, чем текст.

– Слабым звеном ИБ практически любой организации являются люди, то есть ее сотрудники. Наверное, в условиях цифровизации банковской деятельности таким же слабым звеном являются клиенты. Как быть с этой проблемой?

– Обучать, формировать и повышать культуру кибербезопасности. Говоря о культуре кибербезопасности, мы не говорим лишь о сотрудниках. Клиенты и другие граждане – пользователи благ современного общества – это также наша целевая аудитория в данном вопросе.

Сегодня действительно мы продолжаем наблюдать рост социальной инженерии: по нашим данным, на текущий момент она составляет 81% от всего мошенничества на клиентов банка. Именно поэтому мы регулярно проводим мероприятия по повышению киберграмотности наших клиентов, наших юных будущих клиентов и всех граждан, которые пользуются Интернетом, социальными сетями, посещают публичные мероприятия. В социальных сетях регулярно публикуются посты по схемам социальной инженерии и методам противодействия им, в мобильном приложении "Сбербанк Онлайн" размещаются рекомендации по правилам кибербезопасности – каждая коммуникация охватывает от 100 до 500 тысяч человек.

Особая роль в формировании культуры кибербезопасности отводится детям. Именно у них есть то самое необходимое время, чтобы выработать привычку жить в мире, в котором возник новый вид угроз – киберугрозы, и эффективно от них защищаться. Проведение обучающих семинаров и конкурсов, разработка обучающих программ в игровой форме привлекают внимание детей и помогают популяризировать тему кибербезопасного поведения в современном обществе. Работа с детьми при этом

доставляет особое удовольствие. Например, к 30 ноября – Международному дню защиты информации – мы проводили конкурс детских рисунков "Кибербезопасность глазами детей" среди детей наших сотрудников. Удивительные рисунки мы получили: родители объяснили или для начала даже уточнили для себя, что такое кибербезопасность, дети пропустили информацию через свой фильтр важности и сфокусировали наше внимание на самых ключевых темах, волнующих пользователей.

В моменты живого диалога со своей целевой аудиторией ты понимаешь, что твое дело важно и ценно для безопасности современного общества, и хочется продолжать развиваться, улучшать и продвигать культуру кибербезопасности.

– Какие способы и методы обучения культуре кибербезопасности являются, на ваш взгляд, наиболее эффективными?

– Самые эффективные, на наш взгляд, методы обучения – это симуляция жизненных ситуаций (киберучения), баннеры и плакаты, микрообучения, а также обучающие игры. Именно эти методы в комплексе стали для нас новым и эффективным направлением повышения осведомленности.

– Как выстроен процесс обучения непосредственно в Сбербанке?

– Комплексно. Что я имею ввиду: выявив самые эффективные методы обучения с учетом особенностей современного обучаемого, мы осознаем, что каждый человек индивидуален и восприятие разных методов обучения у людей разное, – это раз. Чем больше мы задействуем внимание обучаемого, тем больше шансов на успех, – это два.

У нас запущен единый для всего банка обучающий курс с элементами геймификации, охватывающий все основные правила кибербезопасности. Его проходят все сотрудники, без исключений. Кроме этого, знания, полученные в курсе, мы усиливаем, проверяем, углубляем.

Одним из самых распространенных видов атак, с которыми сталкиваются наши сотрудники, является социальная инженерия, поэтому мы проводим регулярные киберучения – симуляции, имитирующие такие атаки. Мы ежемесячно размещаем скринсейверы по правилам КБ, регулярно проводим коммуникации по внутренним каналам взаимодействия по отдельным кейсам, требующим внимания. Мы обучаем наших коллег требованиям КБ и правилам в форме коротких обучающих роликов.

Регулярные киберучения охватили более 280 тысяч сотрудников банка и его дочерних компаний, которым были направлены учебные фишинговые письма, подброшены фишинговые флешки и совершены "мошеннические" телефонные звонки. Если при проведении первых киберучений в 2016 году по фишинговой ссылке прошли 48% сотрудников, то в мае 2018 года – 1,6%.

Обязательную для всех сотрудников банка flash-игру "Агент кибербезопасности", которая направлена на повышение киберкультуры, прошли почти все сотрудники банка.

Все способы обучения мы синхронизируем между собой по темам и тем самым разными подходами идем к одной цели – повысить культуру кибербезопасности наших сотрудников.

– Как поколения Y, Z воспринимают необходимость процесса обучения и какие методы являются здесь самыми действенными? Вообще с какого возраста необходимо прививать культуру кибербезопасности?

– Методы, описанные мной выше, это как раз про обучение поколения Y. Многие из его представителей не сталкивались сами с кибермошенничеством и иными кибератаками, и чтобы замотивировать их на обучение, приходится проявлять все навыки аргументации и постоянно прокачивать свои скиллы в этом направлении.

С поколением Z все иначе. Киберпространство – это их пространство. Когда мы проводим семинары для детей, удивляют два момента. Первый – их прокачанность по многим кибервопросам: они живут этим, изучают это и даже поучают своих родителей. Второй момент – каждый раз я удивляюсь количеству фишинговых СМС, которые они могут показать у себя в телефоне, и озвученных кейсов, в которых они сталкивались с кибермошенничеством. Поэтому их не нужно заставлять учиться: они поглощают информацию, которую вы им даете, и проявляют к теме кибербезопасности огромный интерес.

Чем раньше вы начнете погружать своего ребенка в правила кибербезопасности, тем прочнее привычку следовать им в жизни вы сформируете.

– Если говорить о завтрашнем дне культуры кибербезопасности, то каким он может быть (должен быть)?

– Здесь есть четкая картинка желаемого будущего культуры кибербезопасности: специалисты кибербезопасности и дети на уровне привычки руководствуются правилами кибербезопасности в своей деятельности и выступают "проводниками" культуры кибербезопасности, обучая своих близких. В обществе признаются приоритетными правила кибербезопасности и обозначается их значимость для сохранения стабильного развития общества. Тренд роста социальной инженерии падает год от года, потому что все меньше и меньше остается кибербезграмотных людей. Несколько утопично, вам кажется? Но задумайтесь: ведь это и станет результатом формирования киберкультуры как проактивного метода противодействия кибермошенничеству. ●

Ключевая задача для группы Сбербанк

Наращивание масштаба бизнеса, повышение прибыльности и эффективности при одновременном увеличении гибкости, скорости и клиентоориентированности на основе внедрения новых технологий и воспитания нового качества людей.

Международное рейтинговое агентство Brand Finance подготовило рейтинг ведущих брендов по итогам 2018 г. За прошедший год индекс силы бренда увеличился с 90 до 93 пунктов – в результате Сбербанк стал самым сильным банковским брендом в мире. Помимо лидерства в банковской категории, Сбербанк вошел в топ-3 самых сильных мировых брендов, уступив только Ferrari. Стоимость бренда Сбербанк за 2018 г. выросла с $11,6 до $12,4 млрд.

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru