Информационный таргетинг

Таргетинг

- – это направленная реклама, основанная на персонализированной информации о конкретном человеке.
- Существуют компании, которые, используя специально разработанные базы данных, помогут вам вычислить идеального клиента.
- Допустим, вы считаете, что ваш потенциальный клиент – дама средних лет, со стабильным доходом, замужняя (ваша косметическая серия включает также предложения для мужчин «Хороший подарок вашему любимому»).
- Ваши пожелания загружают и получают адреса потенциальных подходящих клиентов. Отослав свои рекламные послания именно по этим адресам, вы, скорее всего, получите отклик, если не 100%, то в любом случае хороший.

Виды таргетинга

- *Подбор рекламных площадок*. Наиболее популярный вид таргетинга. Осуществляется путем подбора рекламных площадок так, чтобы их посетители соответствовали целевой аудитории.
- *Тематический таргетинг*. Показ рекламы на веб-сайтах, соответствующих определенной тематике.
- *Таргетинг по интересам* (контекстная реклама). Показ рекламы в соответствии с интересами посетителей рекламной площадки.
- *Географический таргетинг* (геотаргетинг). Показ рекламы целевой аудитории, ограниченной некоторым географическим регионом, выбранным рекламодателем.
- *Таргетинг по времени показа* (утро или вечер, будни или выходные). Позволяет ограничить показ рекламы по времени в течение дня, недели, года.
- *Социально-демографический таргетинг* по возрасту, полу, доходу, должности и т. д.
- *Ограничение количества показов одному пользователю*, позволяет регулировать количество показов рекламного носителя одному уникальному пользователю в процессе его взаимодействия с рекламной площадкой. Чаще всего применяется в баннерной рекламе с оплатой за 1000 показов.
- *Поведенческий таргетинг* Самое перспективное направление на сегодняшний день Суть его сводится к внедрению механизма сбора информации о действиях пользователя в интернете с помощью cookie-файлов. Информация собирается в так называемых профилях и содержит данные о просмотренных сайтах, поисковых запросах, покупках в интернет-магазинах и т.д. Получив такой профиль, рекламная служба может четко представить себе портрет объекта, узнать его привычки и пристрастия, стать владельцем контактных данных.

Прямой и косвенный таргетинг.

- *Прямой* таргетинг нацелен на выбор целевой аудитории, напрямую интересующейся предлагаемым товаром или услугой. *Косвенный* таргетинг нацелен на аудиторию, являющуюся целевой для взаимосвязанных с предлагаемым видом товаров или услуг.
- Уникальную возможность таргетинга предоставляют поисковые системыУникальную возможность таргетинга предоставляют поисковые системы, так как их посетители четко формулируют свою потребность в виде запроса, а также автоматические предоставляют системе некоторые свои характеристики.
- Таргетинг позволяет добиться повышения эффективности рекламного сообщения

Что же включают в себя базы данных?

- Огромное количество информации, как базовой, так и индивидуальной.
- К базовой информации относится, например, демографическая: пол, возраст, наличие машины, дома, тип резиденции, занятость, семейное положение.
  К дополнительной относится, информация о наличии домашних животных, детей, бытовой техники (ее разновидностей: кухонный комбайн, стиральная машина, посудомоечная машина) и так далее.
- В базе данных может содержаться информация о том, пользуется тот или иной клиент кредитной карточкой, ужинает ли он дома или предпочитает ходить в ресторан, голосовал ли он на прошлых выборах и участвовал ли в переписи населения. Если клиент является постоянным посетителем спортивных клубов или салонов красоты, это тоже может проявиться в базе данных. Там может находиться информация о том, жертвовал ли ваш потенциальный клиент на нужды благотворительности и как он относится к деятельности «зеленых».

Цель базы данных

- – подобраться к потенциальному клиенту настолько близко, насколько он сам позволит.

Откуда берется информация

- Конечно же, эта информация не берется с потолка.
- На Западе все давно привыкли к тому, что различные фирмы проводят анкетирование.
- Наградой за заполненную анкету, может быть какой-нибудь небольшой сувенир или розыгрыш в лотерее.
- Человек обычно дает какую-нибудь информацию о себе, когда получает кредитную карточку или открывает счет банке (по крайней мере свое имя и адрес).
- Так что все легально и на благо потребителей, ну и, разумеется, тех, кто занимается рекламной рассылкой.

Факторный анализ

- По каждому фактору можно сделать обобщающий вывод, то есть, насколько этот фактор характерен для базы данных в целом.
- То есть, сколько процентов из базы данных курит, незамужем или живет в отдельном доме.
- Таким образом, вы можете сразу понять, подходит ли вам эта база данных.
- Например, искомый фактор – количество автомобилей в семье. Тогда, если ваша рассылка рассчитана на промоушн машинного масла, вам нужно ориентироваться на семью хотя бы с одной машиной.
- А если вы продаете сами машины, то нужно ориентироваться на средний доход семьи в целом. Это же правило касается и фандрайзинга.
- Если вы намерены собирать пожертвования на восстановление храма, возможно, особое внимание следует уделить факторам «вероисповедание» и «предыдущая благотворительная деятельность».

Соседский таргетинг (Neighboring)

- На Западе существует также некая разновидность таргетинга – направленная на жильцов соседских домов (Neighboring), когда 50-100 человек, живущих по соседству, получают рекламные послания несущие скрытый посыл:
- «Дорогая Миссис N. Хотим сообщить вам, что ваш сосед из дома 45 по улице Грин уже воспользовался новой услугой нашей фирмы».
- Это апелляция к соседским чувствам работает на Западе, поскольку люди, которые живут по соседству (чаще всего средний класс) обычно пользуется одними и теми же банками, ходят в одни и те же магазины, зачастую в одну и ту же церковь (всю эту информацию можно почерпнуть из базы данных).

Фишинг-атаки – преступление 21-го века.

- **В отчете за январь 2007 года по данным Anti-Phishing Working Group (http://www.anti-phishing.org/) приводятся следующие цифры:**

Количество уникальных фишинговых атак	**29930**
Количество уникальных фишинговых сайтов	**27221**
Количество торговых марок, похищенных фишерами в январе	**135**
Страна, в которой в январе было открыто максимальное количество фишинговых сайтов	**США**
Содержащих некоторую часть подлинного имени сайта в адресе	**24.5 %**
Никакого имени, только IP-адрес	**18 %**
Процент сайтов, не использующих 80-й порт	**3.0 %**
Среднее время активности сайта	**4 дня**
Максимальное время активности сайта	**30 дней**

Фактор социальной инженерии

- **Phishing нападения полагаются на соединение методов технического обмана и факторов социальной инженерии.**
- **В большинстве случаев Phisher должен убедить жертву преднамеренно выполнить ряд действий, которые обеспечат доступ к конфиденциальной информации.**
- **В настоящее время фишеры активно используют популярность таких средств связи как электронная почта, web-страницы, IRC и службы мгновенной передачи сообщений (IM).**
- **Во всех случаях Phisher должен являться олицетворением доверенного источника (например, службы поддержки соответствующего банка и т.д.), чтобы внушить доверие жертве.**

Методы, используемые фишерами при работе с электронной почтой:

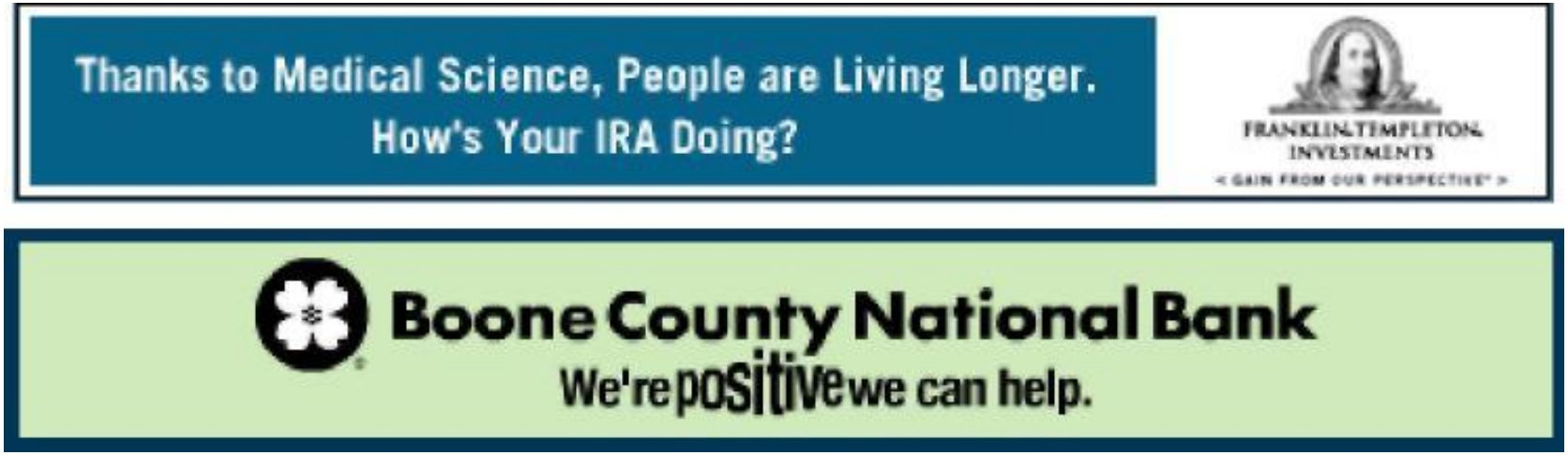
- **Официальный вид письма;**
- **Копирование законных корпоративных адресов электронной почты с незначительными изменениями URL;**
- **HTML, используемый в электронных сообщениях, запутывает информацию об URL;**
- **Стандартные вложения вируса/червя в сообщения;**
- **Использование технологий запутывания анти-спамовых фильтров;**
- **Обработка "индивидуализированных" или уникальных почтовых сообщений;**
- **Поддельные отсылки по почте к популярным доскам объявлений и спискам адресатов;**
- **Использование поддельной строки “Mail From:” адреса и открытые почтовые релеи маскируют источник электронной почты.**

Фишинг-атаки с использованием web-контента

- **Все более и более популярный метод фишинг атак заключается в использовании злонамеренного содержания web-сайта. Это содержание может быть включено в сайт фишера, или сторонний сайт.**
- **Доступные методы доставки контента включают:**
- **Включение HTML замаскировывающее ссылки в пределах популярных сайтов;**
- **Использование сторонних включений или заголовов рекламных банеров для соблазнения клиентов к посещению фишерского сайта;**
- **Использование дефектов сети (скрытые элементы в пределах страницы - типа графического символа нулевого размера), чтобы проследить потенциального клиента в подготовке к нападению фишеров;**
- **Использование всплывающих, чтобы замаскировать истинный источник фишерского сообщения;**
- **Внедрение злонамеренного содержания в пределах просматриваемой web-страницы, которая эксплуатирует известную уязвимость в пределах программного обеспечения web-браузера клиентов и устанавливает программное обеспечение фишера (например, троянские программы).**

Фальсификация рекламных банеров

- **Реклама с помощью банера - очень простой метод фишинга. Он может использоваться для переадресации клиента к поддельному сайту организации.**



•Пример рекламного баннера

IRC и передача IM-сообщений

- **Сравнительно новым является использование IRC и IM-сообщений. Однако, вероятно, этот способ станет популярной основой для фишинг-атак. Так как эти каналы связи все больше нравятся домашним пользователям, и вместе с тем в данное ПО включено большое количество функциональных возможностей, то количество фишинг-атак с использованием этих технологий будет резко увеличиваться.**
- **Вместе с тем необходимо понимать, что многие IRC и IM клиенты учитывают внедрение динамического содержания (например графика, URL, мультимедиа и т.д.) для пересылки участниками канала, а это означает, что внедрение методов фишинга является достаточно тривиальной задачей.**
- **Общее использование ботов[3] во многих из популярных каналов, означает, что фишеру очень просто анонимно послать ссылки и фальсифицировать информацию предназначенную потенциальным жертвам.**

Использование троянских программ

- **В то время как среда передачи для фишинг-атак может быть различна, источник атаки все чаще оказывается предварительно скомпрометированным домашним ПК. При этом как часть процесса компрометации используется установка троянского ПО, которое позволит фишеру (наряду со спамерами, программными пиратами, DDoS ботами и т.д.) использовать ПК как распространителей вредоносных сообщений. Следовательно, прослеживая нападение фишеров, чрезвычайно сложно найти реального злоумышленника.**
- **Необходимо обратить внимание на то, что несмотря на усилия антивирусных компаний, число заражений троянскими программами непрерывно растет. Многие преступные группы разработали успешные методы обмана домашних пользователей для установки у них программного обеспечения и теперь используют большие сети развернутые с помощью троянского ПО (на сегодняшний день не редкость сети составляют сети состоящие из тысяч хостов). Данные сети используются, в том числе, для рассылки фишинговых писем.**
- **Однако не стоит думать, что фишеры не способны к использованию троянских программ против конкретных клиентов, чтобы собирать конфиденциальную информацию. Фактически, чтобы собрать конфиденциальную информацию нескольких тысяч клиентов одновременно, фишеры должны выборочно собирать записываемую информацию.**

Троянские программы для выборочного сбора информации

- **В начале 2004, фишеры создали специализированный кейлоггер. Будучи внедрен в пределах стандартного сообщения HTML (и в почтовом формате и на нескольких скомпрометированных популярных сайтах) он был кодом, который попытался запускать Java аплет, названный “javautil.zip”. Несмотря на свое расширение zip, фактически это был исполняемый файл, который мог быть автоматически выполнен в браузерах клиентов.**
- **Троянский кейлоггер был предназначен для фиксирования всех нажатий клавиш в пределах окон с заголовками различных наименований, включающих:-commbank, Commonwealth, NetBank, Citibank, Bank of America, e-gold, e-bullion, e-Bullion, evocash, EVOCash, EVOcash, intgold, INTGold, paypal, PayPal, bankwest, Bank West, BankWest, National Internet Banking, cibc, CIBC, scotiabank and ScotiaBank.**

Методы противодействия фишинговым атакам

- **Как может обычный пользователь противостоять атаке фишеров? На самом деле, стоит задуматься над несколькими правилами:**
- **Никогда не отвечайте на письма, запрашивающие вашу конфиденциальную информацию**
- **Посетите веб-сайт банка путем ввода его URL-адреса через адресную строку браузера**
- **Регулярно проверяйте состояние своих онлайн-счетов**
- **Проверьте уровень защиты посещаемого вами сайта**
- **Проявите осторожность, работая с электронными письмами и конфиденциальными данными**
- **Обеспечьте защиту своему компьютеру**
- **Всегда сообщайте об обнаруженной подозрительной активности**