ГЛОБЭКС БАНК

Снижение рисков, связанных с человеческим фактором

Алябьев Андрей

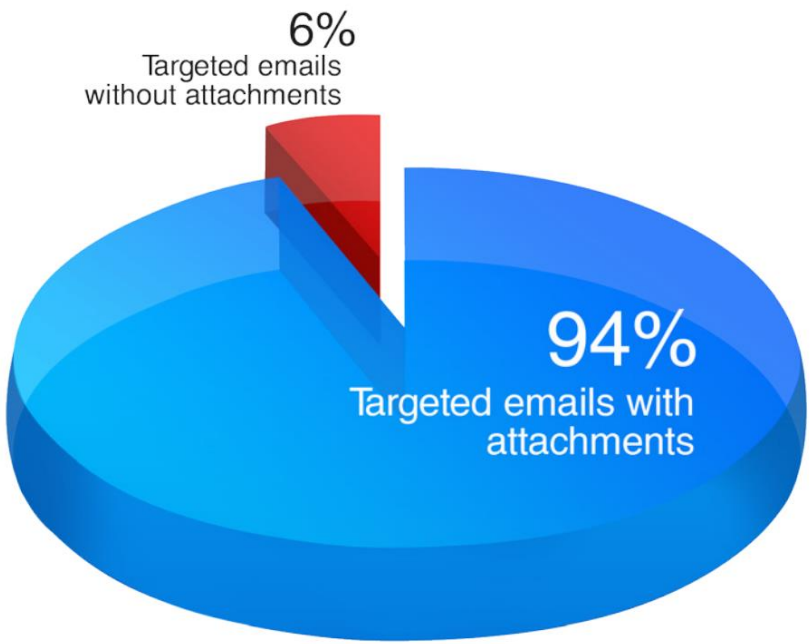
Отдел информационной безопасности

10 ноября 2016

Почему это важно

TREND MICRO™ Research Team:

91-percent of hacking attacks begin with a phishing or spear-phishing email



Какая ситуация в банках

«За отчетный период FinCERT зафиксировал значительное число атак, связанных с подменой входных данных для АРМ КБР (изменение содержимого XML-документа, используемого для формирования электронного сообщения, направляемого в Банк России). Атака производилась по следующей схеме:

1. В большинстве случаев в кредитную организацию злоумышленниками направлялось электронное письмо, содержащее вредоносное ПО, не детектируемое антивирусными средствами…»

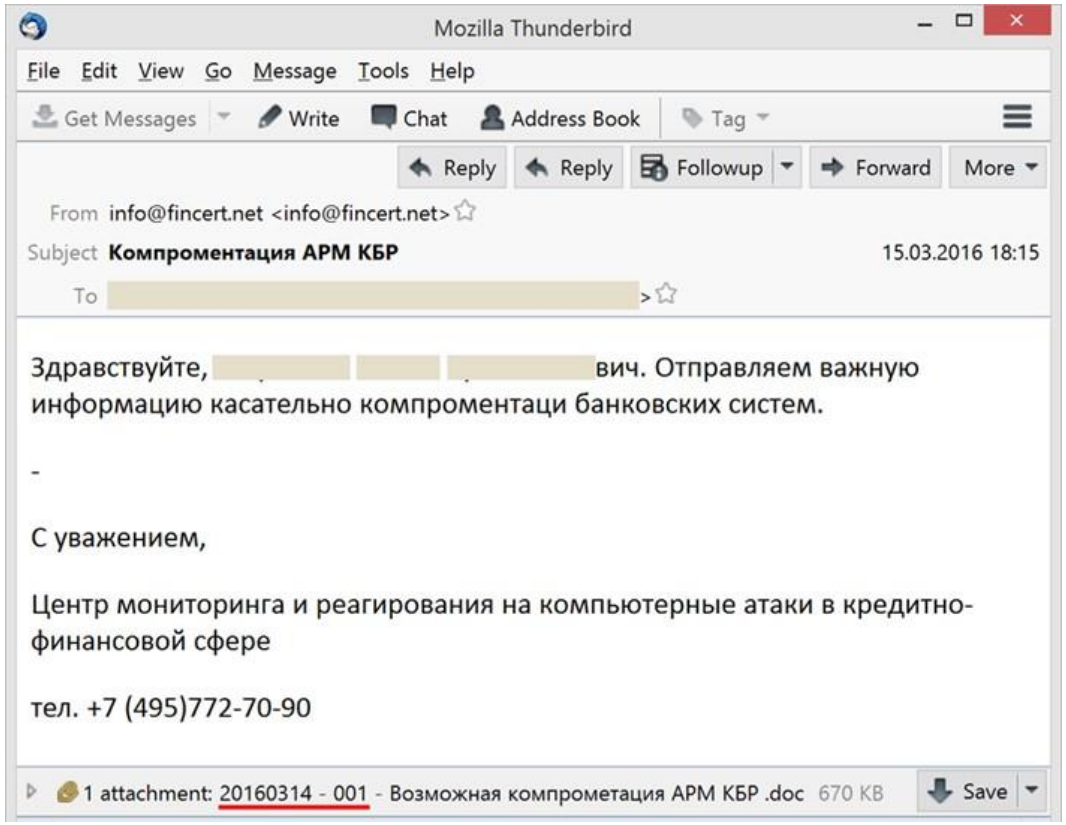
Как выглядит хорошее фишинговое письмо

Отправители

- Органы исполнительной власти;
- Крупные телекоммуникационные операторы;
- Профильные интернет-форумы;
- Кредитно-финансовые организации;
- Организации-партнеры;
- Организации-клиенты.

Содержание

- Требование, поступившее от органов исполнительной власти;
- Рассылка изменений в нормативных актах;
- Взыскание/погашение задолженности/штрафа, оплата услуг;
- Поиск документов для проверки.



Обучение

Проект по выстраиванию процесса повышения осведомленности

- Ответственные, сроки, бюджет проекта
- Программа обучения
- Разработка материалов / выбор готовой системы

Проводим обучение:

- Базовая программа для новых сотрудников
- Периодические рассылки по отдельным темам
- Разовые рассылки с важной информацией об актуальных угрозах

Проверяем :

- Оценка знаний
- Тестирование в «боевых» условиях»

Рынок систем повышения осведомленности

Figure 1. Magic Quadrant Security Awareness Computer-Based Training

Source: Gartner (October 2015)

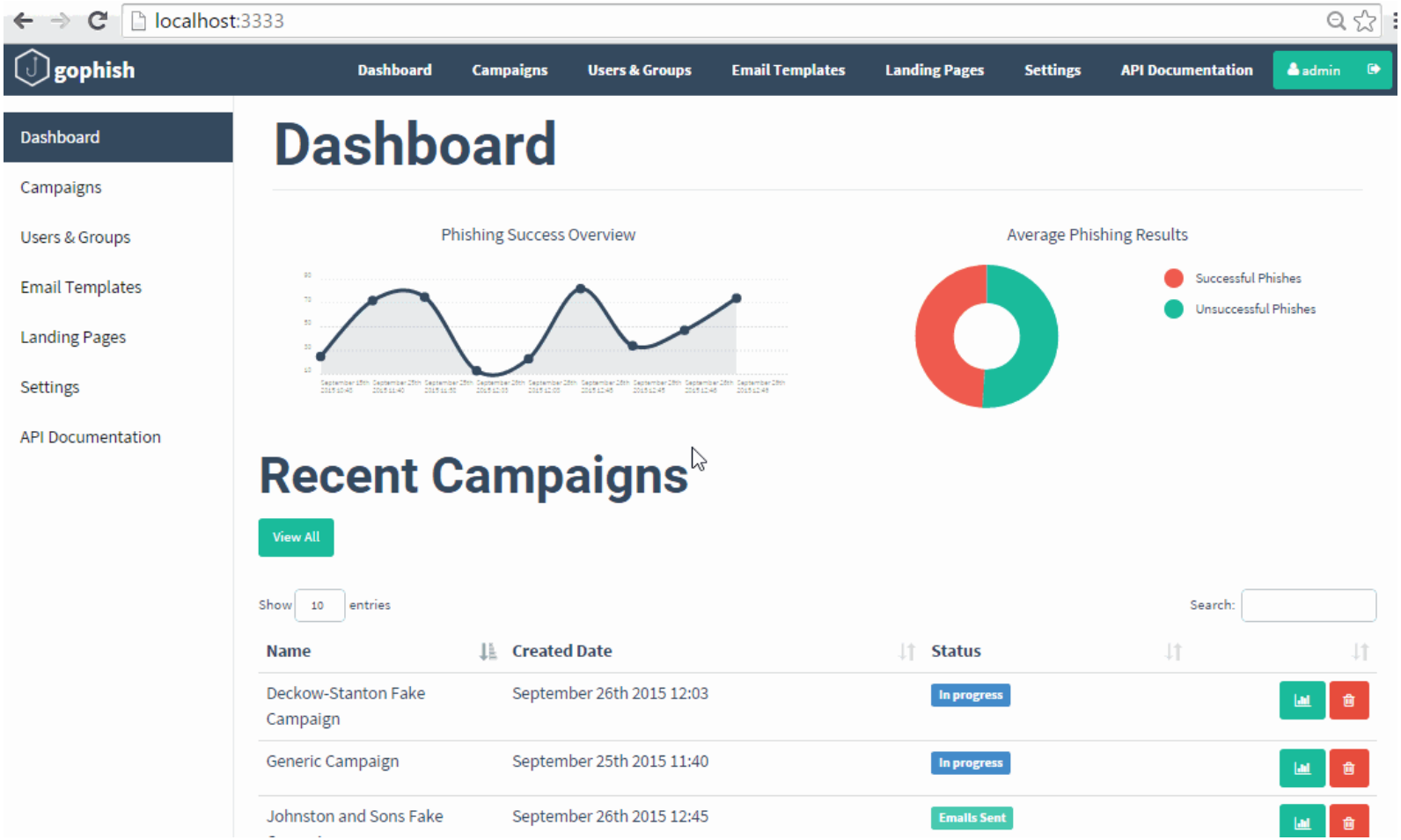
Как повысить эффективность обучения?

имитировать действия злоумышленника:
фишинговые рассылки в учебных целях

Фишинговые рассылки: варианты реализации

Решение	Описание	Плюсы	Минусы
Аутсорсинг	Услуга популярна и предлагается многими компаниями (в первую очередь теми, кто занимается pentest'ом)	Простота и доступность услуги. Идеально для однократного теста	Дороже, чем самостоятельная реализация
Самостоятельно: без использования готовой платформы	Полностью «ручное» решение: регистрируем домены, поднимаем почтовый сервер, организуем трекинг открытия вложений	Мы ограничены только фантазией и ресурсами	Большие трудозатраты, сложно анализировать результаты
Система on-site 	Установка готового решения на своей площадке. Автоматизируем большую часть операций по рассылке. Есть инструменты для анализа результатов	Простота развертывания, дашборды и статистика	Ограничен функционал: нет трекинга вложений, нет своего почтового сервера
Облачное решение SecurityIQ PHISHME	Регистрация на сайте компании разработчика и получение доступа к личному кабинету, из которого настраиваются рассылки	Функциональность, простота, возможность интеграции с системой обучения	Передача третьим лицам чувствительной информации.

gophish


localhost:3333
gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Settings
API Documentation
admin
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Settings
API Documentation
Dashboard
Phishing Success Overview
Average Phishing Results
Successful Phishes
Unsuccessful Phishes
Recent Campaigns
View All
Show 10 entries
Search:
Name
Created Date
Status
Deckow-Stanton Fake Campaign
September 26th 2015 12:03
In progress
Generic Campaign
September 25th 2015 11:40
In progress
Johnston and Sons Fake
September 26th 2015 12:45
Emails Sent

gophish

Details

Show 10 entries Search:

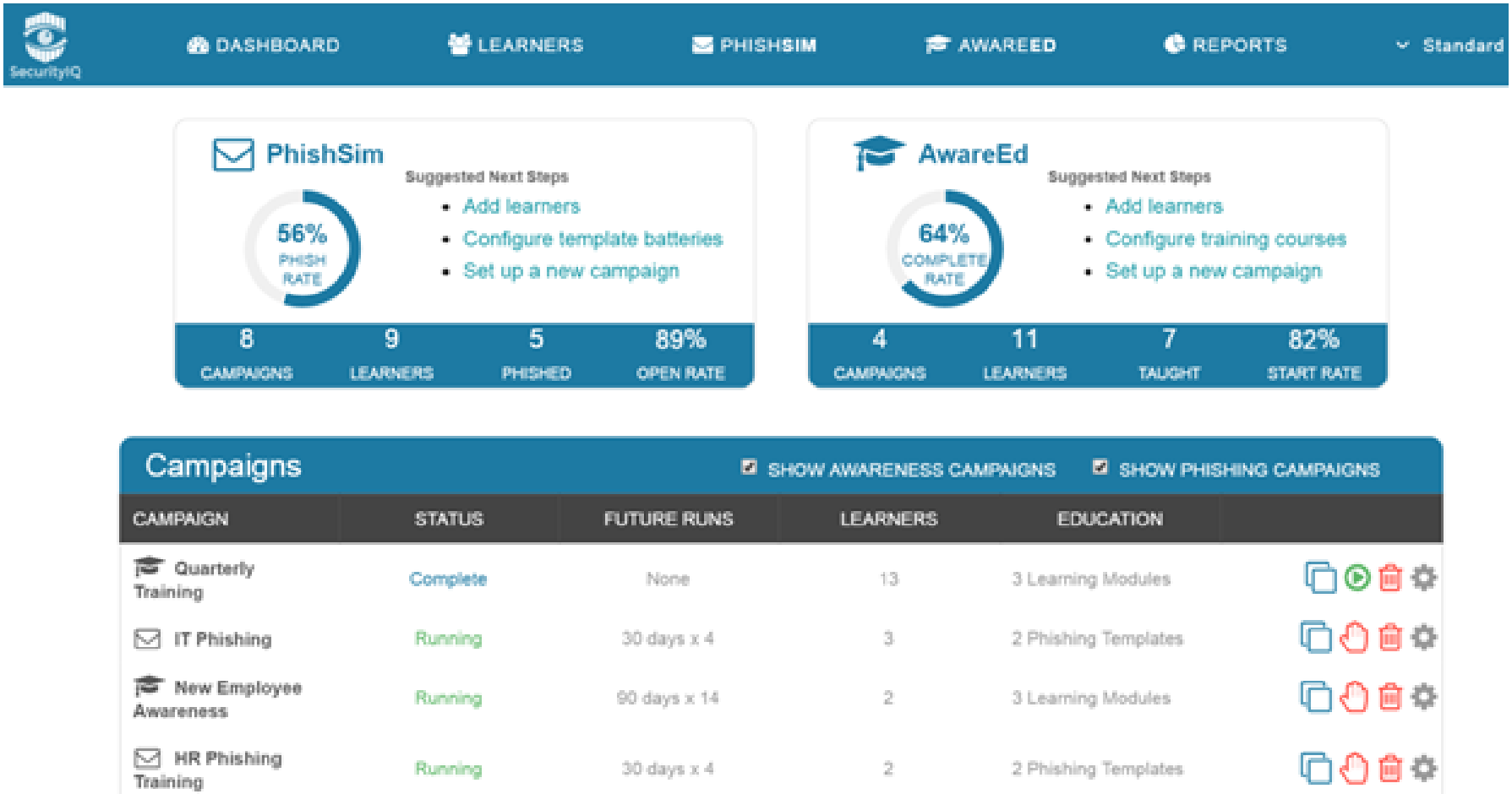
	First Name	Last Name	Email	Position	Status
▸	jordan	wright	jordan@example.com		Error
▾	test	test	test@test.com		Success

Timeline for test test

Email: test@test.com

- Campaign Created — *January 24th 2016 8:00*
- Email Opened — *January 29th 2016 9:26*
- Clicked Link — *January 29th 2016 9:26*

SecurityIQ by Infosec Institute (phish.io)



SecurityIQ by Infosec Institute Institute (phish.io)

Campaign Run Details

Run	Status	Start	End	Length	Learners	Templates	Open Rate	Phish Rate
1	Complete	10/27/2016	10/28/2016	1 Days	6	1	67%	33%

Sends

Date	Learner	Template	Status	Trained
10/27/2016	[redacted]@globexbank.ru	Рассылка от компании ЦФТ	Phished and Opened Attachment	Not Started
10/27/2016	[redacted]@globexbank.ru	Рассылка от компании ЦФТ	Phished and Opened Attachment	Not Started
10/27/2016	[redacted]@globexbank.ru	Рассылка от компании ЦФТ	Sent	N/A
10/27/2016	[redacted]@globexbank.ru	Рассылка от компании ЦФТ	Sent	N/A
10/27/2016	[redacted]@globexbank.ru	Рассылка от компании ЦФТ	Opened	N/A
10/27/2016	a.alyabiev@globexbank.ru	Рассылка от компании ЦФТ	Opened	N/A

Итоги

Угрозы, связанные с использованием социальной инженерии, в ближайшем будущем никуда не денутся (а скорее всего, будут только расти)

- Такие атаки универсальны для проникновения в любые системы, легко тиражируются
- Достаточно одного «попавшегося» для компрометации всей сети
- Не стоит полагаться исключительно на технические средства

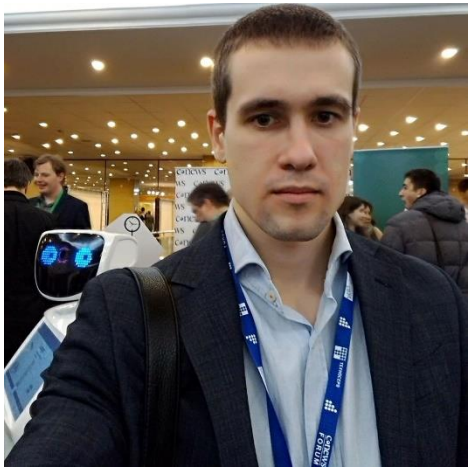
Можно снизить риски, обучая сотрудников и эффективно проверяя их знания

- Дополняем организационные меры «боевыми учениями»
- Тестирование путем проведения фишинговых рассылок можно дополнять имитацией других действий злоумышленников: телефонное мошенничество, тесты на проникновение

Важно не то, какими именно инструментами мы пользуемся, а качественно организованный процесс обучения и тестирования

- Все приведенные решения – всего лишь частные примеры реализации
- Если процессов нет, то и нечего будет автоматизировать

Спасибо за внимание



Мои контакты:
Алябьев Андрей
a.alyabiev@globexbank.ru
+7 (495) 691-75-07

https://facebook.com/andrey.alyabiev

https://ru.linkedin.com/in/andreyalyabiev