

Как за 1 день внедрить систему  
оценки осведомленности  
сотрудников?

# Актуальность проблемы

«Целью большинства атак со стороны хакеров являются люди, а не технические уязвимости.»

**Symantec Security Response**

«Врожденной» защиты от фишинга нет ни у одной платформы — это по-настоящему универсальная угроза.»

**Лаборатория Касперского**

«Социальная инженерия используется в каждой третьей атаке на компании».

**Positive Technologies**

# Устанавливаем Gophish

The image shows a promotional page for Gophish on the left and a laptop displaying the Gophish dashboard on the right.

**Website Content:**

- Logo: Gophish
- Navigation: Документация, Служба поддержки, Блог, [Скачать](#)
- Section Header: **Фишинговая платформа с ОТКРЫТЫМ ИСХОДНЫМ КОДОМ**
- Description: Gophish - это мощная фишинговая среда с открытым исходным кодом, которая позволяет легко проверить подверженность фишинга вашей организации.
- Text: Бесплатно.
- Buttons: [Скачать](#), [Подробнее](#)

**Dashboard Content (on laptop):**

- Header: gophish
- Section: Dashboard
- Chart: A red area chart showing trends over time.
- Metrics: Four circular progress indicators for Email Sent, Email Opened, Clicked Link, and Submitted Data.
- Section: Recent Campaigns
- Table: A table with two rows of campaign data, each row having a green bar and a red bar.

# Что потребуется для внедрения системы Gophish

- Сервер
- Немного ~~нервов~~ времени вашего it-специалиста
- Тексты писем
- Таблица с сотрудниками

# Как написать письмо

Главное правило: ввести в заблуждение

1. С *чем* связана деятельность сотрудника
2. С *кем* связана деятельность сотрудника

# Таблица с сотрудниками

3	Имя	Фамилия	Email	Должность
4	Любовь	[REDACTED]	[REDACTED]	Секретарь
5	Василий	[REDACTED]	[REDACTED]	Бухгалтерия
6	Алексей	[REDACTED]	[REDACTED]	Бухгалтерия
7	Гейдар	[REDACTED]	[REDACTED]	Бухгалтерия
8	Сергей	[REDACTED]	[REDACTED]	Менеджер
9	Семен	[REDACTED]	[REDACTED]	Менеджер
10	Вячеслав	[REDACTED]	[REDACTED]	Менеджер
11	Дмитрий	[REDACTED]	[REDACTED]	IT-специалист

# Результаты использования

- Тестовая группа 117 человек
- Письмо с «вредоносным» файлом – 20% попавшихся
- Многоходовая атака – 40% попавшихся

Другач Юрий [www.facebook.com/yuresd](http://www.facebook.com/yuresd)

Блог о социальной инженерии [icast.ru](http://icast.ru)