The Security Company International

INSPIRE. ENGAGE. PROTECT.

CASE STUDY /
Diary of an identity theft victim – awareness campaign

colt
smarter / faster / further

The Security Company (TSC) delivered a communications campaign to encourage Colt's employees to be cautious online. This supported Colt in raising awareness of advanced persistent threats.

Background

Following the increase in advanced persistent threat attacks witnessed during 2011, Colt commissioned an attack against itself to test how prepared it was. The findings revealed that employees felt they could trust the majority of electronic communications, whether or not they knew the sender. This left them vulnerable to risks such as clicking on links or attachments contained in emails.

Objectives

- To tackle the 'false trust' amongst Colt employees.
- To make employees aware that electronic communications cannot be guaranteed to be genuine.
- To encourage employees to think before they click.
- To address the following topics:
  - Secure passwords
  - Phishing attacks
  - Computer viruses
  - Loose talk/Disclosing information on social networks
  - Social engineering
  - ID theft

Delivery

Colt commissioned a third party to create two characters, a victim and a social engineer. The characters had no obvious differentiators (gender, culture, etc.) to show that anyone can appear trustworthy.

The characters inspired the development of the 'Diary of an identity theft victim'. Four diary entries detailed a typical day's events in which the author puts their personal and company information at risk online via social networks. The final instalment focussed on the consequences of the victim's unsecure actions. The campaign was delivered on a weekly basis via the Security Portal site, supported by an email that linked through to the campaign.

Online banners

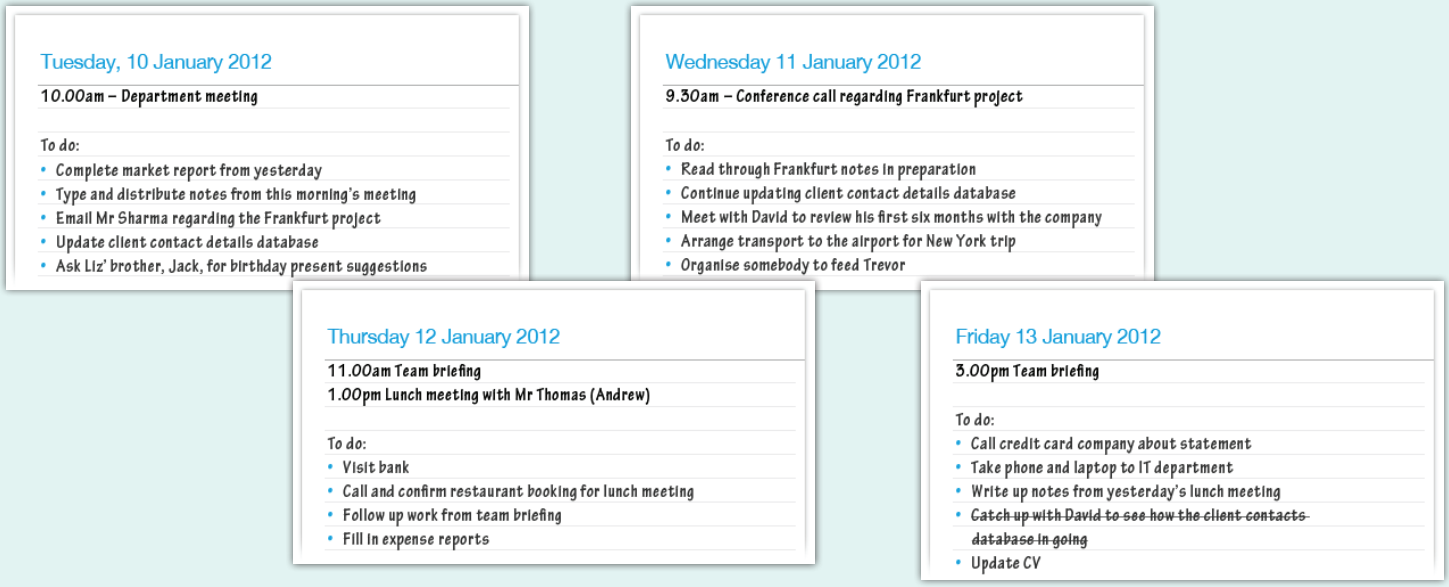
Day one

Day two

Day three

Day four

The diary entries:



Tuesday, 10 January 2012

10.00am – Department meeting

To do:
- Complete market report from yesterday
- Type and distribute notes from this morning's meeting
- Email Mr Sharma regarding the Frankfurt project
- Update client contact details database
- Ask Liz' brother, Jack, for birthday present suggestions

Wednesday 11 January 2012

9.30am – Conference call regarding Frankfurt project

To do:
- Read through Frankfurt notes in preparation
- Continue updating client contact details database
- Meet with David to review his first six months with the company
- Arrange transport to the airport for New York trip
- Organise somebody to feed Trevor

Thursday 12 January 2012

11.00am Team briefing
1.00pm Lunch meeting with Mr Thomas (Andrew)

To do:
- Visit bank
- Call and confirm restaurant booking for lunch meeting
- Follow up work from team briefing
- Fill in expense reports

Friday 13 January 2012

3.00pm Team briefing

To do:
- Call credit card company about statement
- Take phone and laptop to IT department
- Write up notes from yesterday's lunch meeting
- ~~Catch up with David to see how the client contacts database is going~~
- Update CV

The challenges

The original brief required a formal tone of voice to illustrate a business diary, written from a woman's point of view. Reconsidering the objective to encourage secure behaviour at home and at work and the requirement to engage a predominantly male workforce, the brief was amended and the character was determined as male.

It was important to retain the reader's interest and urge them to spot the victim's mistakes using their judgement. Each diary entry included a link to more information detailing the behaviour that led to the victim having their identity stolen and offering advice on how to avoid the same situation.

The outcome

Site hits allowed us to measure the success of this campaign. During the month the campaign was delivered, unique user visits to the Security Portal increased by 236%. In addition, a maximum of 84% of recipients opened the emails used to promote the campaign.

"I've worked with The Security Company for a number of years and appreciate their creativity and ideas. I've been particularly impressed by the imaginative way they manage to bring important security messages to life in a way that immediately captures the attention of the employee audience. This recent campaign regarding the dangers of sharing information online proved very popular with our workforce who were fully engaged. The campaign's outcome was 100% successful in relation to employee awareness and cultural change expectations."

Jim Mulheron - Vice President Security and Operational Risk Group, Colt