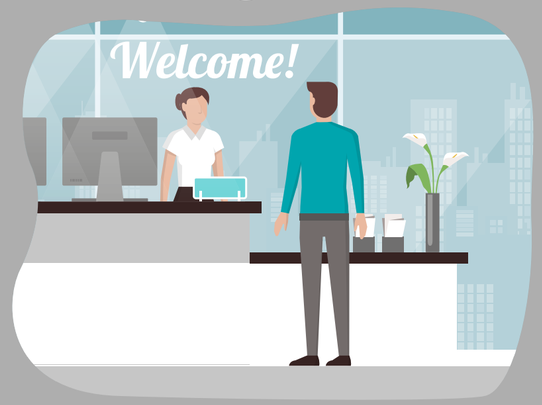
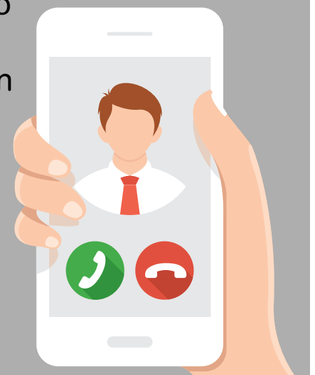
## Step I:
## Identifying a Target

FIN7 targets companies: particularly fast-food and casual-dining restaurants, hotels, casinos, and those with a high frequency of point-of-sale transactions. FIN7 gathers information to develop messaging similar to the company's routine business communications.

## Step 2:
## Grooming




Spear phishing e-mails target victim company employees: typically public-facing contacts, like employees handling catering requests and reservations, and/or in a managerial position. FIN7 accompanies the e-mails with telephone calls to persuade the employee to open and activate the e-mail's attachment, which contains malware.



## Step 3:
## Infiltrating System

a) Once activated, the malware allows FIN7 to connect to the computer, download additional malware, and move through the company's network. The malware allows FIN7 to conduct surveillance on company employees, capturing credentials to gain elevated network access.

b) FIN7 locates the Point of Sale systems containing customer data and steals caches of payment card numbers.


## Step 4:
## Selling Stolen Cards

Stolen payment card information resurfaces in online underground marketplaces. Purchased card numbers enable criminals to make unauthorized charges to unsuspecting cardholders. Charges may include typical retail purchases as well as the purchase of gift cards.


# FIN7 Malware Scheme