THE SOCIAL ENGINEER TOOLKIT

TrustedSec's **Social Engineer Toolkit (SET)** is a powerful open-source framework designed for social engineering engagements.

Crafted by David Kennedy (**@HackingDave**), **SET** emphasizes the significance of social engineering awareness in defensive cybersecurity.

Get ready. Get SET. Go!

```
        ..######..########.########
        .##....##.##.........##...
        .##.......##.........##...
        ..######..######.....##...
        .......##.##.........##...
        .##....##.##.........##...
        ..######..########....##...

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                        Version: 8.0.3
                     Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About
```

SET is native to most recent Kali Linux builds.

Download is available for Windows Subsystem for Linux (WSL/WSL2).

```
sudo apt install set -y
```

If download is required, there is also support for other Linux distributions as well as Mac OS X.

Note: SET for Mac OS X is still experimental.

```
$ git clone https://github.com/trustedsec/social-engineer-toolkit/ setoolkit/
$ cd setoolkit
$ pip3 install -r requirements.txt
$ python setup.py
```

SET enables and automates a variety of social engineering attacks.

```
  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules
```

Spear-Phishing: E-mail attacks aimed at *specific* individuals.

Website Attack: Exploiting web applications such as with cross-site scripting (XSS) or SQL injection

Infectious Media: Creating malicious USB/CD/DVD payloads.

Mass Mailer Attack: Large-scale phishing campaigns.

Arduino-Based Attack: Leveraging *Arduino* microcontrollers to create physical devices capable of carrying out cyber attacks.

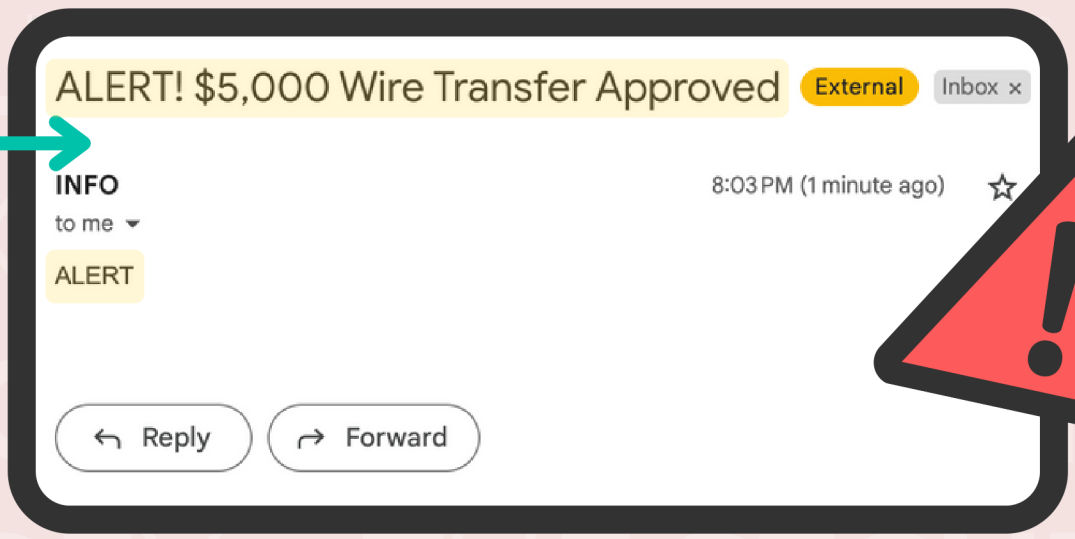
What exactly is *social engineering*?

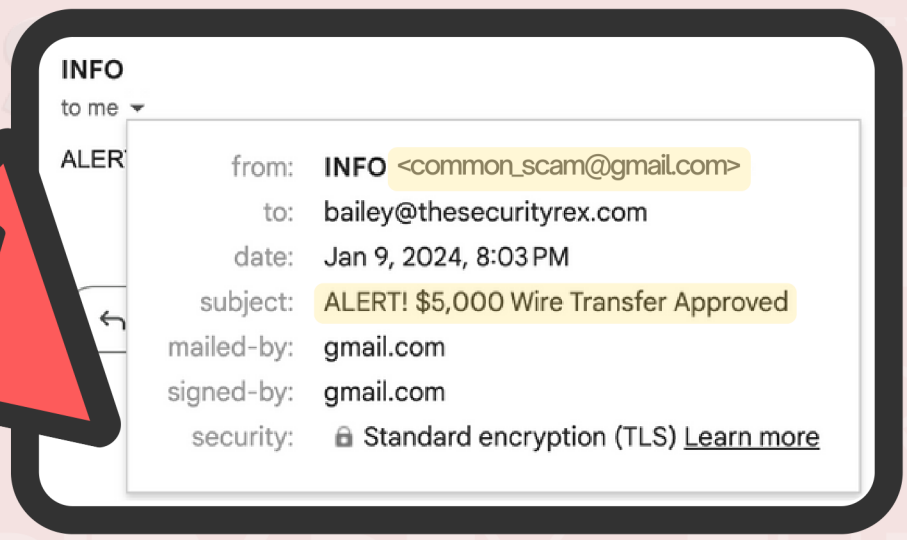
Social engineering involves manipulation with psychological tactics to obtain sensitive information or gain unauthorized access.

EXAMPLE : SELECT *5) Mass Mailer Attack*

```
set>5

  Social Engineer Toolkit Mass E-Mailer

  There are two options on the mass e-mailer, the first would
  be to send an email to one individual person. The second option
  will allow you to import a list and send it to as many people as
  you want within that list.

  What do you want to do:

  1. E-Mail Attack Single Email Address
  2. E-Mail Attack Mass Mailer

  99. Return to main menu.

set:mailer>1
set:phishing> Send email to:bailey@thesecurityrex.com
```

```
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:common_scam@gmail.com
set:phishing> The FROM NAME the user will see:INFO
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:ALERT! $5,000 Wire Transfer Approved
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:ALERT
Next line of the body: END
[*] SET has finished sending the emails

   Press <return> to continue
```





SET also integrates the **Fast-Track Penetration Testing platform** which streamlines the process of setting up and executing attacks.

SCCM Attack Vector: Exploits the Microsoft System Center Configuration Manager.

```
1) Microsoft SQL Bruter
2) Custom Exploits
3) SCCM Attack Vector
4) Dell DRAC/Chassis Default Checker
5) RID_ENUM - User Enumeration Attack
6) PSEXEC Powershell Injection
```

Dell DRAC/Chassis Default Checker: Finds vulnerabilities in Dell's Remote Access Controller or Chassis Management Controller.

RID_ENUM - User Enumeration Attack: Extracts user account information including Security Identifiers (SIDs).

EXAMPLE : SELECT *2) CUSTOM EXPLOITS*

```
set:fasttrack>2

Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing Exploits Section. This menu
has obscure exploits and ones that are primarily python driven. This will continue to grow over time.

   1) MS08-067 (Win2000, Win2k3, WinXP)
   2) Mozilla Firefox 3.6.16 mChannel Object Use After Free Exploit (Win7)
   3) Solarwinds Storage Manager 5.1.0 Remote SYSTEM SQL Injection Exploit
   4) RDP | Use after Free - Denial of Service
   5) MySQL Authentication Bypass Exploit
   6) F5 Root Authentication Bypass Exploit
```

Pre-installed third party modules are available, or there is the option to create and integrate your own modules into the framework.

```
1. RATTE Java Applet Attack (Remote Administration Tool Tommy Edition) - Read the readme/RATTE_REA
2. Google Analytics Attack by @ZonkSec
3. RATTE (Remote Administration Tool Tommy Edition) Create Payload only. Read the readme/RATTE-Rea
```

PURPLESEC

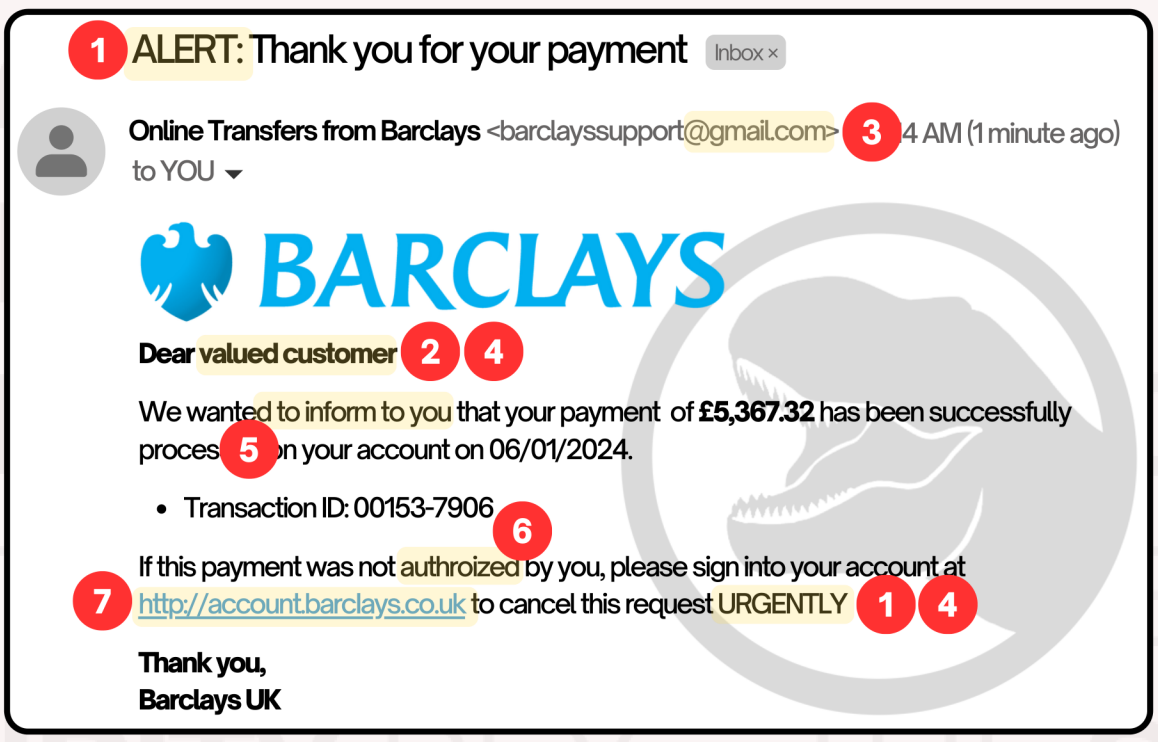
It is reported that 98% of cyber attacks involve social engineering, with ***phishing*** leading to $1.8 billion in annual business losses.

STATISTICS PROVIDED BY PURPLESEC.US

So how do we (really) defend against social engineering?

- Conduct frequent engaging trainings and enforce robust security policies, **extending these requirements to third-party partners**.
- Implement email filtering systems to detect phishing attempts.
- Use email authentication protocols to prevent email spoofing.
- Enforce multi-factor authentication for sensitive systems and data.
- Establish an incident response plan to mitigate the impact of successful attacks.
- Conduct **phishing simulations** to test employees' ability to recognize and resist phishing attempts.

Know what smells phish-y when you open that next email!



1. Sense of urgency
2. No specific name
3. Suspicious address
   A bank would not use a Gmail
4. Poor punctuation
5. Poor grammar
6. Incorrect spellings
7. Suspicious links
   In this link, the "L" in "barclays" is actually a capital "i", and does not use HTTPS