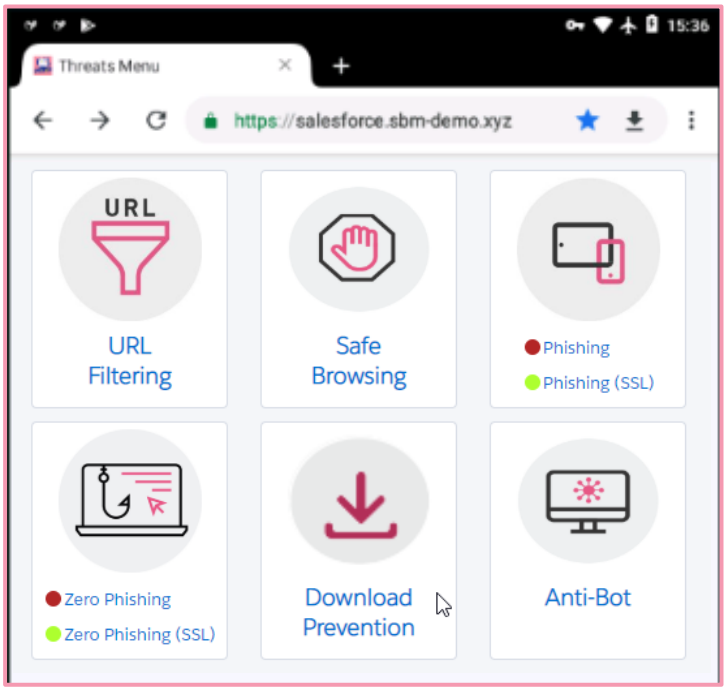
SBM - ONP
Threats Menu
Demo Guide

https://main.sbm-demo.xyz/

How to successfully demonstrate SandBlast Mobile to your customer and partners



Notes:

1. SBM Demo Point Dashboard is set to support this demo page.
2. Partners are welcome to use this demo page.
3. Before using any other dashboard please verify that your dashboard is set as needed, see suggested settings at the end of this guide.

Version 1.3	Minor changes: Page URL + ONP Configuration

URL Filtering

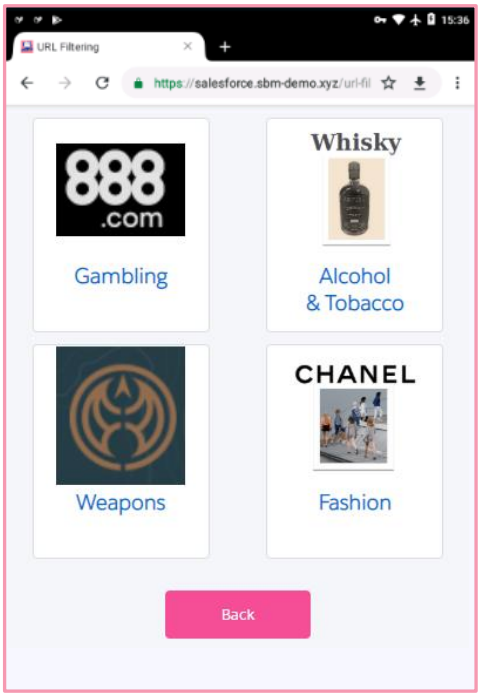
SandBlast Mobile's URL Filtering capability prevents access to websites based on categories deemed inappropriate by the organization's corporate policies.

SandBlast Mobile's URL Filtering technology allows businesses to blacklist and whitelist domains.

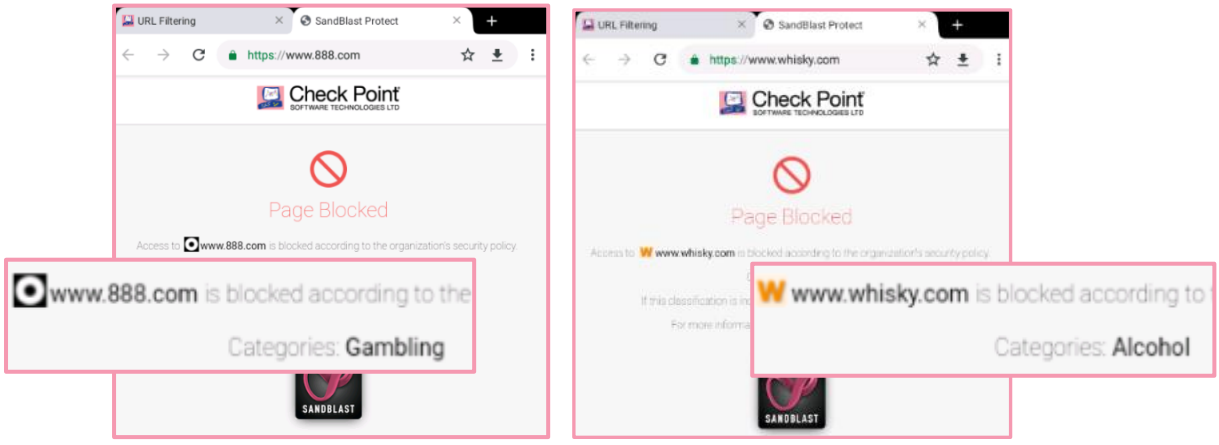
URL Filtering enforces polices on mobile devices across all browser apps and on all non-browser specific apps, such as Facebook Messenger, Slack, WhatsApp and others.

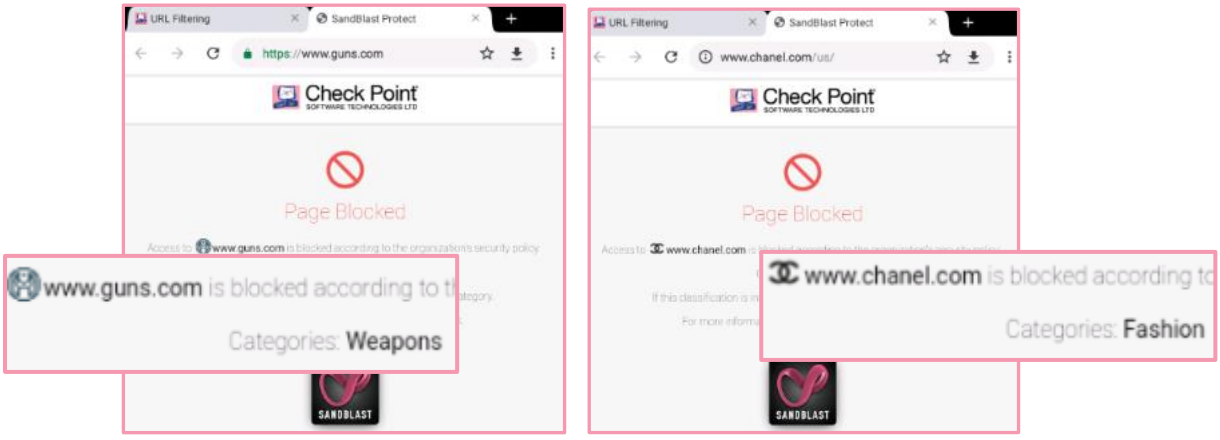
Four different links available, representing the following websites categories:

- Gambling
- Alcohol & Tobacco
- Weapons
- Fashion

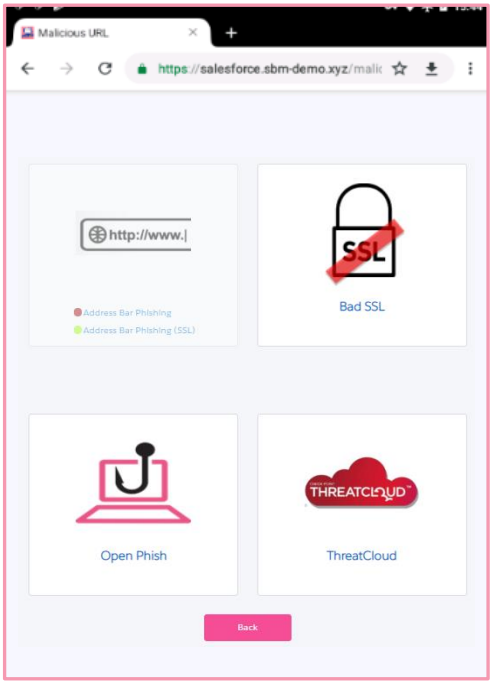


Expected behavior





Safe Browsing



SandBlast Mobile's On-device Network Protection prevents access to malicious websites using any browsing app by blocking access to the site based on dynamic security intelligence provided by ThreatCloud™. Not based on categories but on security indicators.

In addition, it also prevents users from unwittingly visiting malicious websites where their device can be infected with drive-by malware.

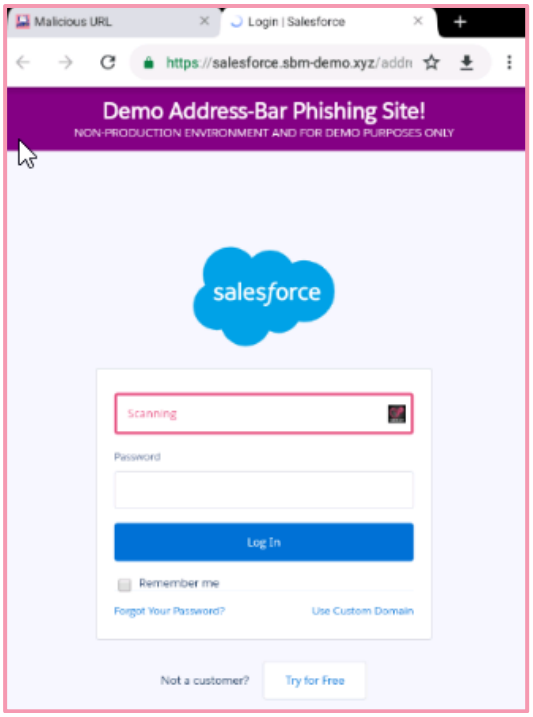
Four different links available,
representing the following attacks:

- **Address Bar Phishing (Http & Https)**
  scam URLs with lookalike text to legit URL
- **Bad SSL**
  Samples of misleading SSL certifications
- **Open Phish**
  3rd party site listing known Phishing URLs
- **Threat Cloud – well known Bot C&C link**
  An internal Check Point test URL listed in the Threat Cloud with as BOT c&c Site

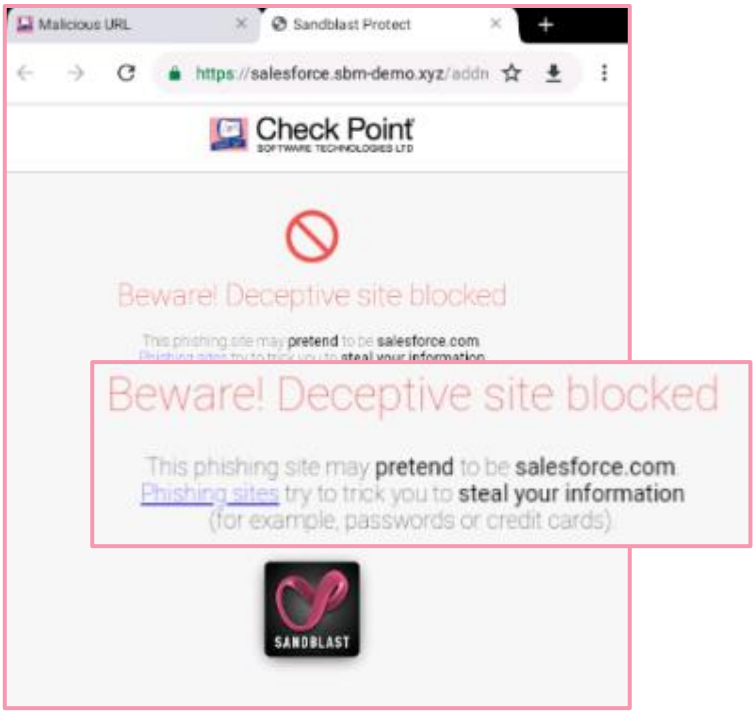
Expected behavior

Address Bar Phishing:

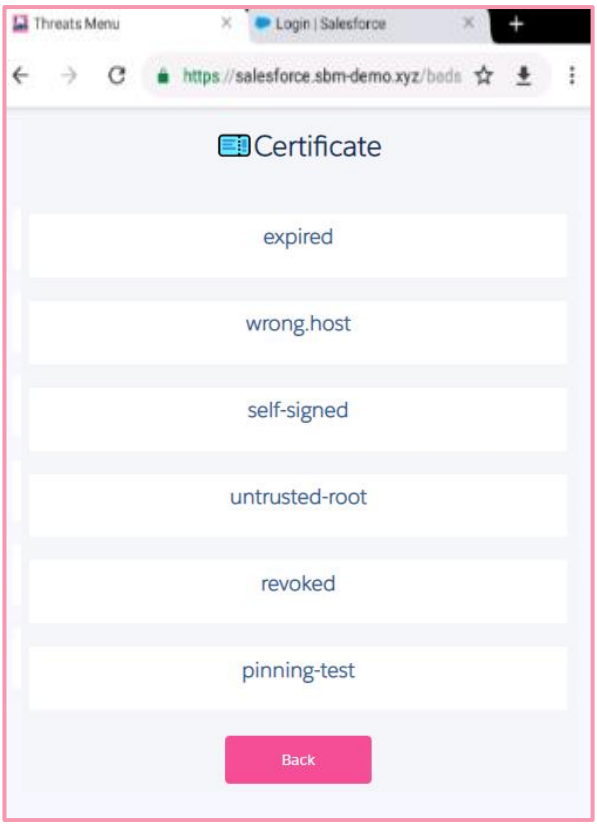
A. Text box Scan



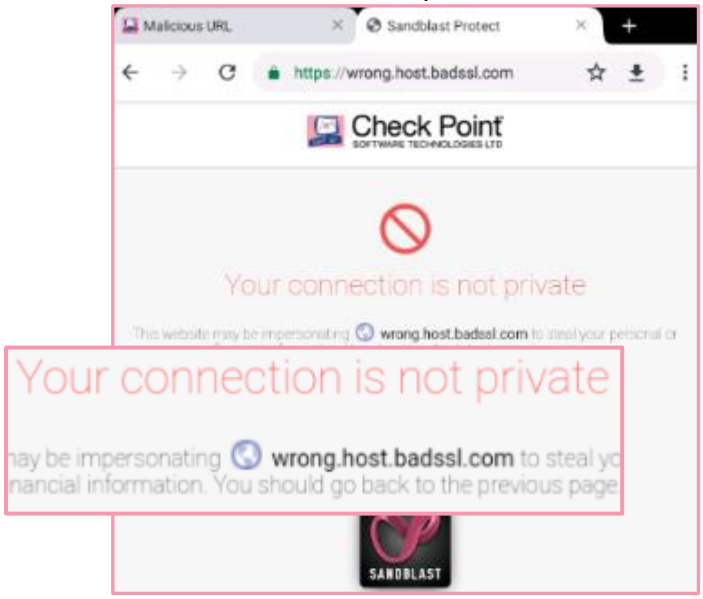
B. Notification page:
"Beware! Deceptive site blocked"

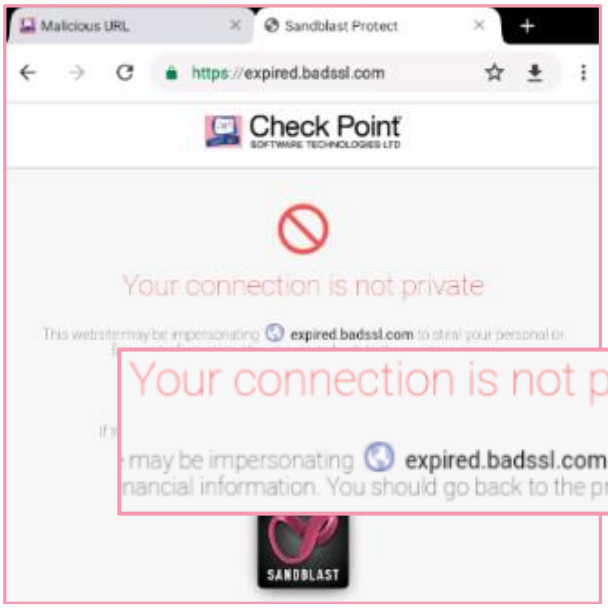


Bad SSL:
Several links for testing clients against bad SSL configurations

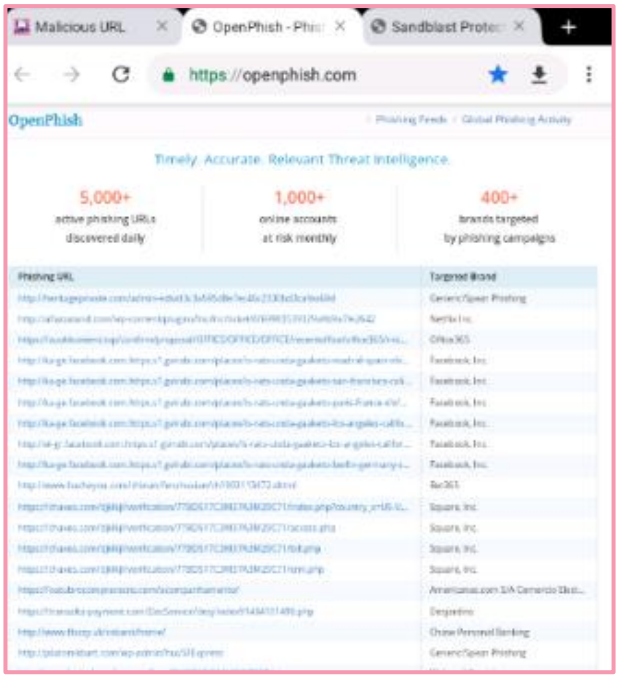


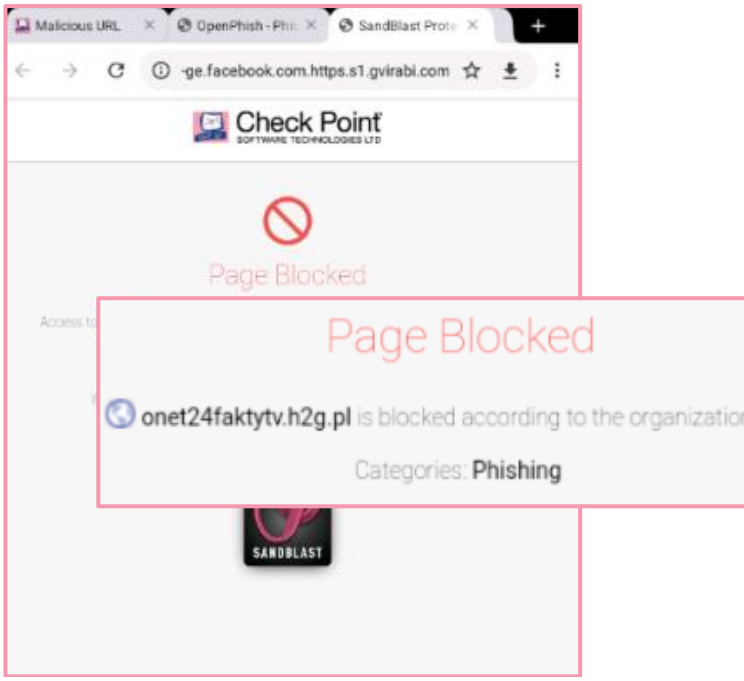
Notification page:
"Your connection is not private"



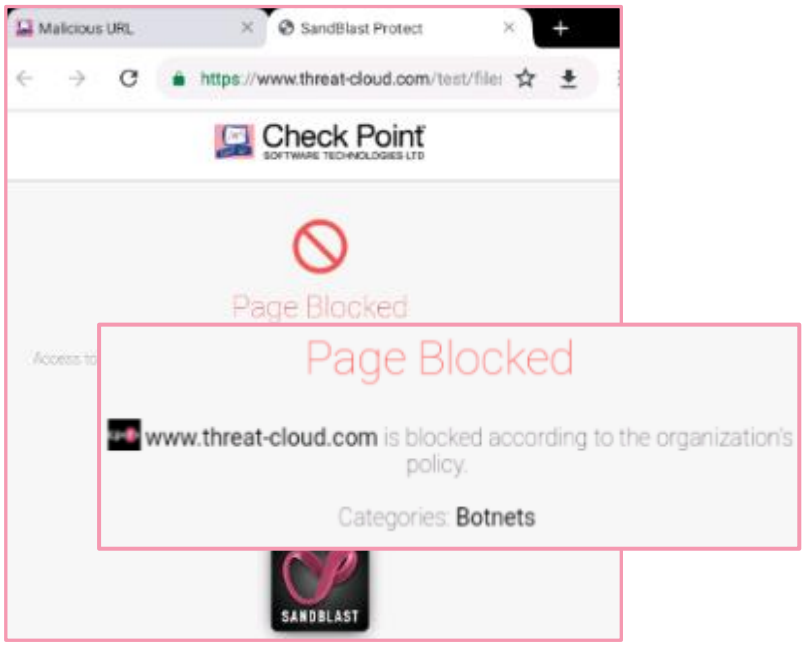


Open Phish:
Page Blocked – Phishing





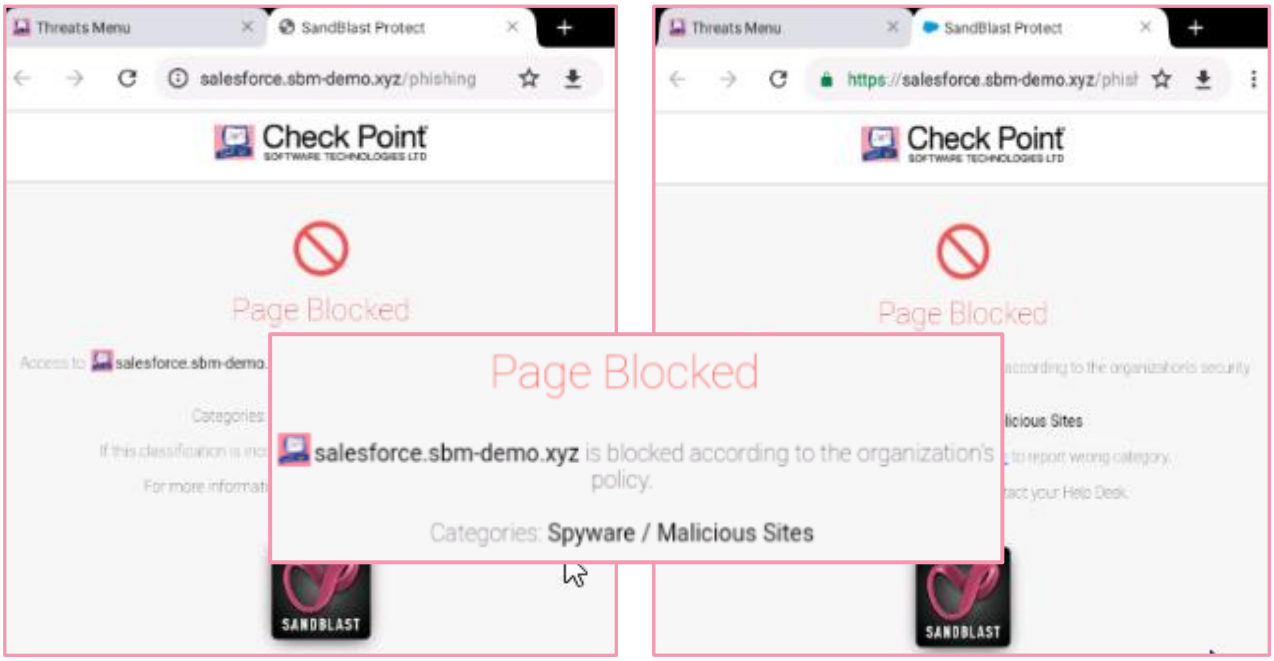
Threat Cloud – well known Bot C&C link
Page Blocked - BOT NET



Phishing & SSL Phishing

Page Blocked - Phishing

Page Blocked – Phishing

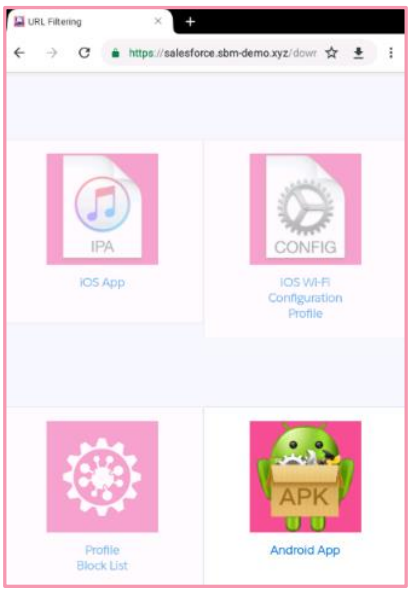


Download Prevention

Links demonstrating 3rd party Application stores (iOS / Android).

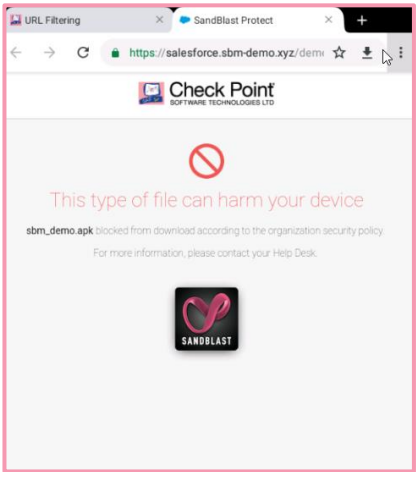
This capability will prevent access to either risky URLs or all 3rd party (except Apple & Google).

Admins may whitelist their corporate stores on the dashboard.



Expected behavior

Notification page:
“This type of file can harm your device”



Zero Phishing

Protecting against Zero Day Phishing sites
This Demo Page supports both HTTP & HTTPS.

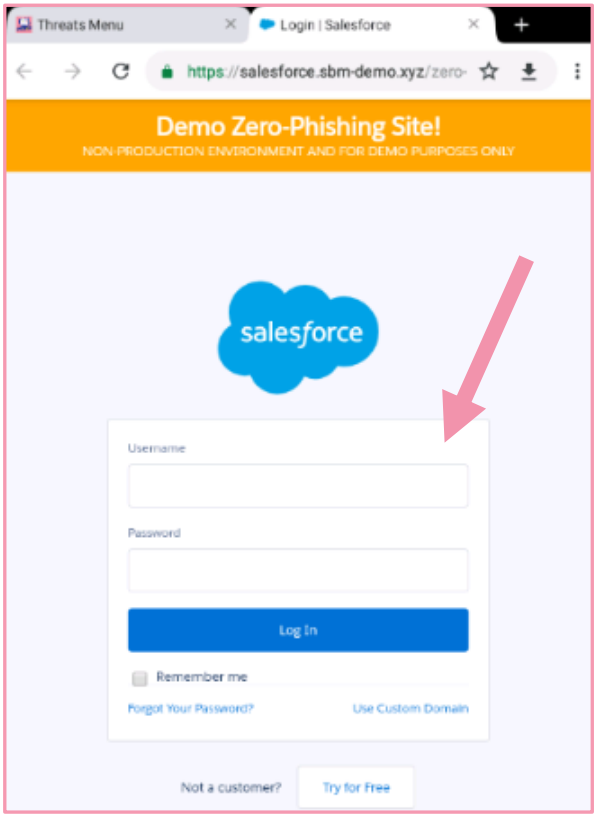
Analyzing Zero Day pages require scanning every unknown website. |
This task creates resource consumption and less than optimal user experience.
In order to alleviate this challenge and make the device more secure and the SandBlast Mobile protect App more efficient we have created the following flow for preventing Zero Day phishing protection.

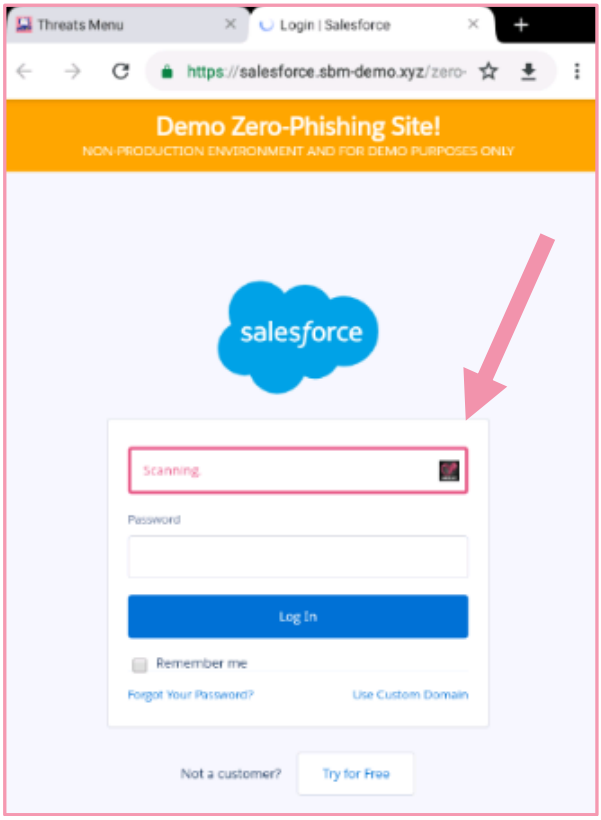
1. As the page loads hidden scan held if the page has input fields in it Y/N
2. If Y, Do we already know this page as legit Y/N
3. If Y (Legit site), No action is done and nothing shown to the user
   (nor in the browser or SBM GUI)
4. If N (unknown site), nothing will happen before selecting one of the text box's
   >>> Upon select,
   security indicators shared with the ThreatCloud and GUI process bar displayed
   >>> Blocking the Page will take place in case malicious verdict response arrived

Note: if we scan URL/Page it is already known.... it is not Zero Day Phishing
(exceptions are our test pages)

Expected behavior

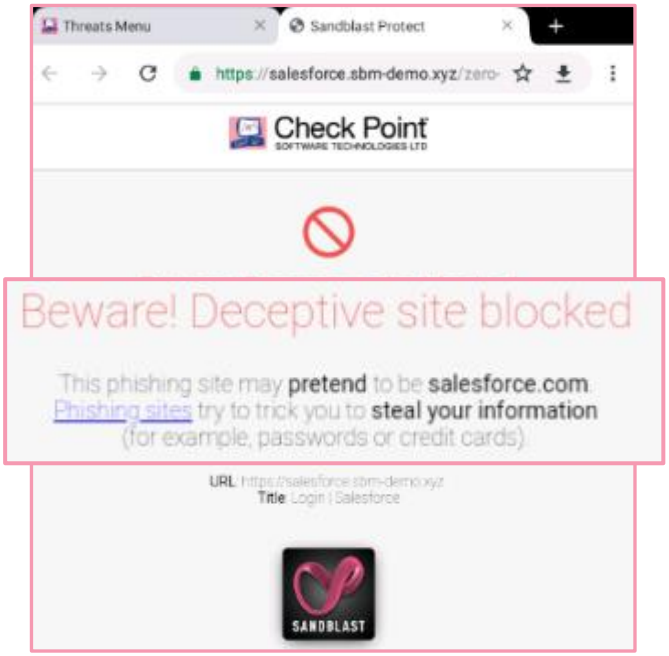
No Action before clicking the text box >>> Scan visualization





After Scan

Notification page: “Beware! Deceptive site blocked”



Suggested Policy Settings: