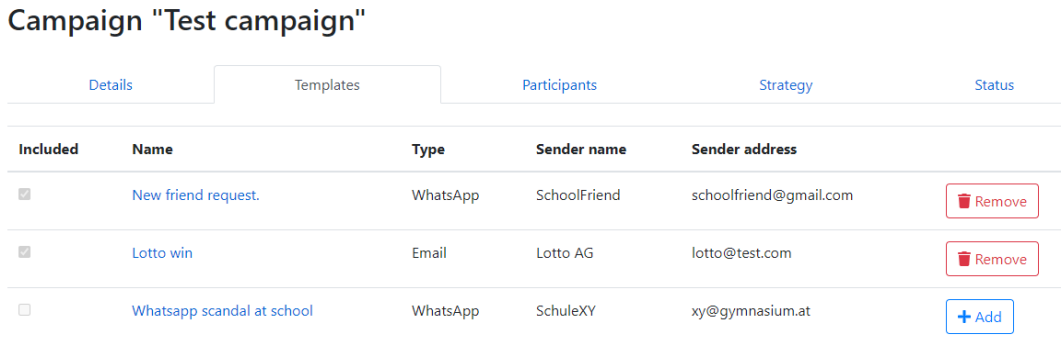
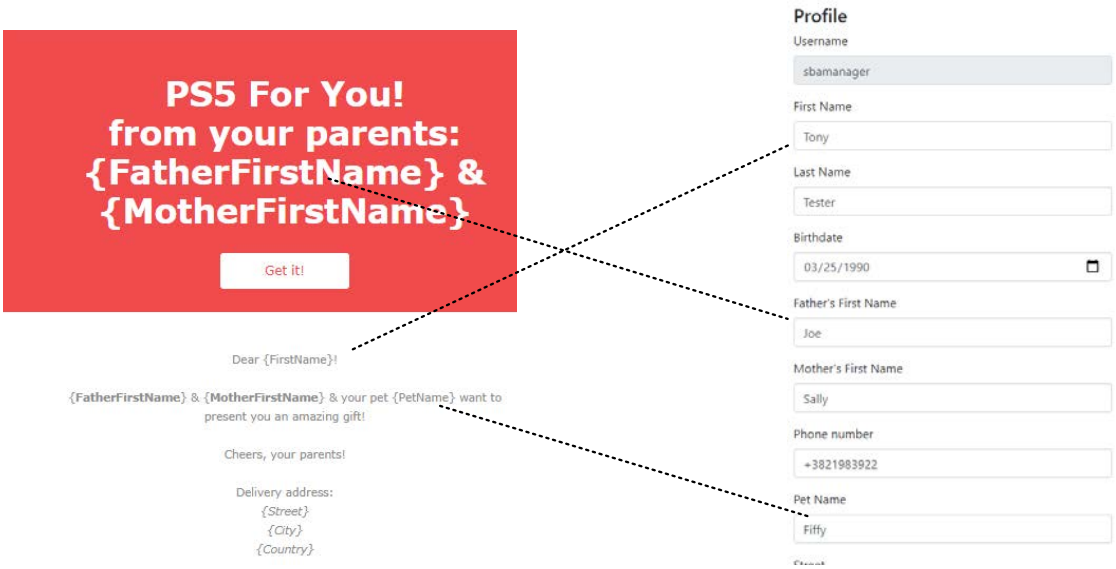
PhishMe App

Eine Kampagne fasst alle Phishing Aktivitäten über einen definierten Zeitraum für eine ausgewählte Teilnehmergruppe zusammen (z.B. eine Schulklasse über 1 Semester).

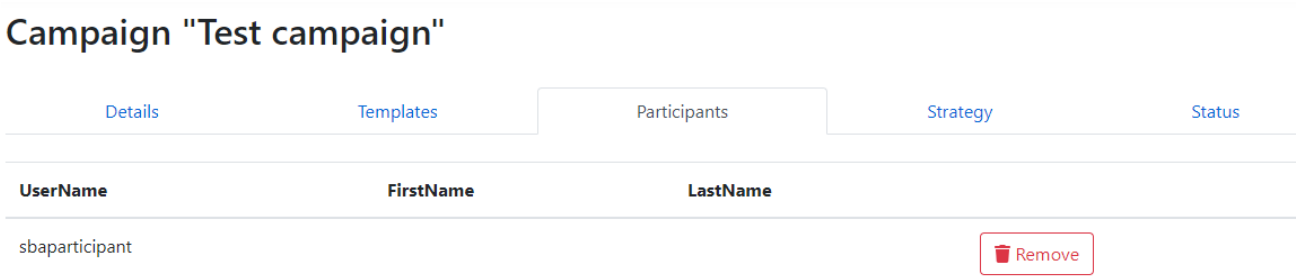
Für die Kampagne werden Phishing Templates ausgewählt (aus einem globalen Pool an definierten Templates – kann man erweitern und wiederverwenden). Jedes Template hat einen definierten Zeitraum/Zeitpunkt, an dem es eingesetzt werden sollte (z.B. 24.12 für ein Phishing-Weihnachtstemplate oder 1.7 bis 1.10 für Schulferien Skandale).
Templates werden für einen bestimmten Channel erzeugt (z.B. E-Mail oder Whatsapp).



Jedes Template beinhaltet auch die eigentliche Nachricht, die versendet werden soll. In dieser Nachricht kann man Placeholder setzen, die mit den Metadaten der Zielperson befüllt wird. Hier ein Beispiel E-Mail Template (.html) und daneben die Metadaten von einem Teilnehmer.



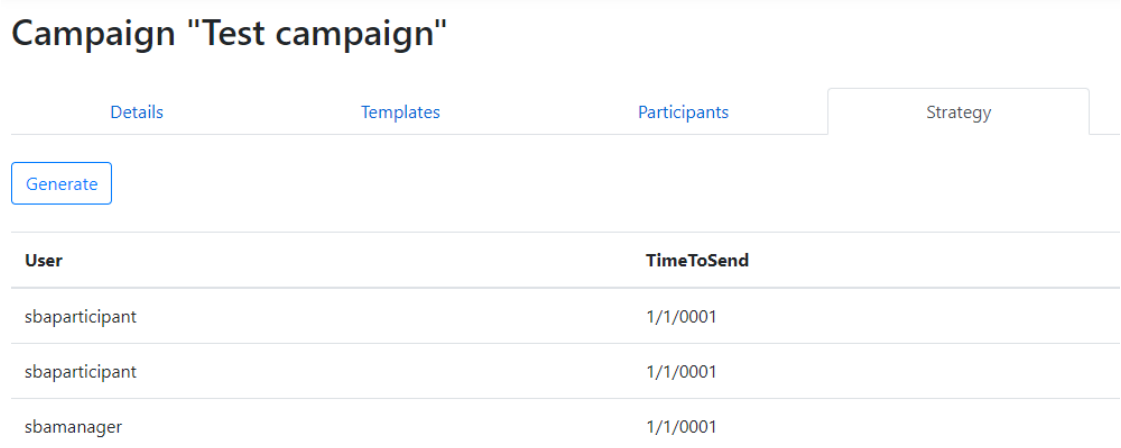
Teilnehmer erhalten einen Kampagne Einladungslink (z.B. vom Lehrer via E-Mail gesendet oder im Unterricht gezeigt), müssen sich dann in der Plattform anmelden und ihre Metadaten befüllen/aktualisieren. Nachdem sie die Einladung bestätigt haben, scheinen sie in der Kampagne als Teilnehmer auf. Wenn die Teilnehmer die Einladung selbst annehmen können wir das vielleicht auch als Zustimmung verwenden – sollten wir entsprechend alle Informationen neben dem Accept Button schreiben.



Als nächsten Schritt möchten wir einen Plan/Kalender erzeugen, in dem alle geplanten Nachrichten über das Semester aufscheinen.

Z.B. wir nehmen das erste ausgewählte Template für die Kampagne, nehmen den ersten Teilnehmer und füllen die Metadataen des Teilnehmers in das E-Mail Template ein. Dann erzeugen wir das geplante Sendedatum (zufällig in dem Zeitraum, den das Template vorgibt – z.B. 24.12 für das Weihnachtstemplate). Dann speichern wir diese konkrete Nachricht mit dem geplanten Sendedatum. Das können wir für jedes Template und jeden Teilnehmer machen, dann haben wir Anzahl Template * Anzahl Teilnehmer Nachrichten.

Der Vorteil von diesem Nachrichten-Plan ist es, dass man hier die Nachrichten noch manuell anpassen könnte für einen bestimmten Teilnehmer (z.B. Sendedatum ändern), löschen, etc.



Wenn der Plan fertig ist, müssen die Nachrichten an dem gesetzten Sendedatum verschickt werden.
Im Hintergrund läuft dafür ein Service, das täglich nachsieht, ob es geplante Nachrichten für den heutigen Tag gibt. Wenn z.B. der 24.12 ist, findet das Service die geplanten Nachrichten für den 24.12 und sendet diese an die entsprechenden Teilnehmer.

Fragen

1. Mit welcher Strategie möchten wir die Nachrichten erzeugen – welche Nachrichten für welchen Teilnehmer. Wirklich jede Nachricht für jeden Teilnehmer – oder eine festgelegte Anzahl (über den Kampagnen-Zeitraum) und zufällig Auswählen für jeden Teilnehmer aus den vorhandenen Templates?

In kommerziellen Phishing Übungen wird häufig dieselbe Nachricht einfach an alle/Mitarbeitergruppe zur selben Zeit geschickt, weil es wie eine Meldung von der Firma aussieht. Bei uns ist das vielleicht weniger sinnvoll, wenn die Schüler sich untereinander austauschen (außer es ist ein Template, das vorgibt von der Schule oder einem Lehrer zu kommen). Für individuelle Templates – wie z.B. deine Eltern schenken dir eine PS5 – ist es verdächtig, wenn jeder Schüler die Nachricht bekommt, dann ist klar, dass es fake ist, sofern sie sich austauschen. Wollen wir das ignorieren oder machen wir genügend Templates, damit nicht alle ident aussehen?
Wenn der definierte Templatezeitraum etwas größer ist, werden die Nachrichten ohnehin an unterschiedlichen Zeitpunkten gesendet für jeden Teilnehmer (Sendedatum wird ja zufällig gewählt).

2. Was machen wir, wenn die benötigten Metadaten für ein Template für einen Teilnehmer nicht eingetragen wurden. Z.B. Template erwartet den Namen des Haustiers aber der Teilnehmer hat kein Haustier eingetragen – unser Vorschlag wäre, diese Templates dann

nicht zu verwenden für den speziellen Teilnehmer. Also die Metadaten bestimmen auch, welche Templates gewählt werden können.

3. Whatsapp automatisiert zu versenden ist wie erwartet nicht so einfach – es gibt die Whatsapp Business API, da muss man sich offiziell anmelden und es steht auf jeder Message, dass es eine Business Message ist (ich vermute unser Zweck ist da ausgeschlossen). Es gibt noch andere APIs aber die laufen alle ähnlich – Twilio zb. geht auch über Business Accounts, andere APIs erfordern, dass man über deren Server sendet – damit würden wir die Daten an sie weitergeben.

Die meisten Freiheiten hätten wir, wenn wir einfach über Selenium oder ähnlich die Klicks auf der Whatsapp WebApp automatisieren. Dann ist es nicht von einem echten Benutzer unterscheidbar – wir benötigen aber echte Sim-Karten und Geräte (man muss auch in der WebApp ab und zu neu verbinden).