Le Phishing pédagogique

Fabrice Prigent

Université Toulouse Capitole

Jeudi 22 juin 2023

L'Université Toulouse Capitole

- Université en droit, économie et gestion, avec une petite UFR informatique,
- 21000 étudiants,
- 2100 personnels (dont 1000 vacataires),
- très forte centralisation (2 entités semi-indépendantes),
- une seule adresse officielle
- un annuaire avec les mails des personnels,
- une unicité du mot de passe,
- une unicité de l'interface de mot de passe (cassification quasi complète).

Définition: le phishing

Phishing: *"L'hameçonnage ou phishing en anglais est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc."*

Définition: le phishing pédagoqique

Le phishing pédagogique est une pratique visant à éduquer et sensibiliser les utilisateurs aux techniques de phishing. Il consiste en la réalisation de simulations contrôlées et préparées de tentatives de phishing, dans le but d'évaluer la vigilance et la préparation des utilisateurs. L'objectif est de former les utilisateurs à reconnaître et à éviter les attaques de phishing réelles, renforçant ainsi la sécurité globale d'une organisation. Le phishing pédagogique doit être réalisé de manière éthique, transparente et avec le consentement des participants. Son but est d'éduquer et de former, et non de causer des préjudices.

Les conséquences d'un phishing

- Un phishing réussi c'est rapidement
  - 1 million de spams qui partent.
  - une porte d'entrée pour des actions plus dangereuses (ransomware, nous voilà !)
- D'où
  - des mises en quarantaine
    - plus ou moins longues
    - plus ou moins visibles
    - les pires étant les invisibles longues (vive les blacklists inconnues)
  - des baisses de réputation (mxtoolbox.com, mail-tester.com)

La pédagogie

Les utilisateurs ne lisent pas les documentations, les newsletters, les notes de services.

Et comment fais-tu pour qu'ils comprennent ?
Des explications, des schémas, une écoute.

Et s'ils ne comprennent toujours pas ?
Des baffes !

Le diplôme ne change rien

J'ai reçu un mail d'eBay me demandant mes coordonnées, alors que je n'ai pas de compte eBay. C'est pour cela que j'ai mis mon mot de passe de la fac.

J'ai bien fait ?

Le principe

La DSI envoie

- à tous les personnels
- aléatoirement
- mais pas plus d'une fois tous les 2 mois
- un mail de phishing
- qui renvoie sur une page quasi-identique à notre mire d'authentification

Objectifs

Nous avions un objectif clair :

Améliorer

Améliorer la résistance de l'ensemble de la communauté UT Capitole aux phishings actuellement en activité.

et SURTOUT PAS

Piéger

Piéger les utilisateurs.

Comment cela a été politiquement mis en place ?

- Un accord de principe de la Direction Générale des Services, suite à une démonstration.
- Une information en CA (ou toute instance représentative)
- Un mail à TOUS signalant la campagne, ses objectifs, etc.

Cela a été facile, mais pensez bien à **différer toute idée de faire un top ten, ou de sanctionner.**

Les thèmes des campagnes

A l'UT Capitole:

- Le thème du quota en début d'année
  - C'est l'échauffement
- Le thème du moment dans les phishing actuels
  - Par fainéantise
  - Systématiquement validée (*Je sais qu'elle est vicieuse, mais les pirates sont en train de la faire*)
- Avec parfois des campagnes "vaccinales d'urgence": tout le monde en moins d'une journée.
  - Si nous sommes suffisamment rapides, le vrai ne les touchera pas
  - Sinon, le "faux" les fera se questionner sur le vrai

Avertir ou pas ?

A l'UT Capitole, avertissement ou pas des campagnes, cela n'a pas d'importance :

- En juillet 2022 : Tout le monde a été prévenu deux semaines en amont des thèmes des trois campagnes à venir.
- Fin Janvier 2023 : Alerte sur le phishing Izly, et annonce d'un phishing sur le thème. 29 piégés. (le record depuis 2015).

Architecture

A l'UT Capitole

- Un script en perl de 260 lignes plus 70 par campagne
- Un serveur web qui envoie de fausses réponses à Google, Bing et consorts.
- Un nom de domaine plausible

Les résultats vis à vis de la campagne pédagogique

- Les nouveaux se font piéger à plus de 50%,
- Les "habitués" sont très résistants (3%), (syndrome de Milgram, et à l'incompréhension des adresses d'expéditeur)
- Certains laissant même des messages au RSSI

Bande de ptits salopiaux. Aucun respect

UNIVERSITÉ TOULOUSE CAPITOLE

Les résultats vis à vis de vrais phishings

Nous sommes passés

- de 5 à 6 piégés par an (avec des machins qui ne ressemblaient à RIEN !)
- à 0-1 par an
  - avec des phishings utilisant notre mire
- ils refusent même de cliquer sur des mails normaux (mais pas toujours bien conçus) de la DSI et du ministère.

Les campagnes qui marchent

L'expérience permet de savoir ce qui piège le plus.

- L'argent
  - primes, chèques vacances, etc.
- Les congés
- Surtout quand c'est agrémenté d'un peu d'actualité.
- Les horaires auxquels vous faites la campagne
  - Heures ouvrées (surtout juste avant d'aller manger !)
  - Jours ouvrés *"Les informaticiens ne travaillent jamais le dimanche"*
- En faisant par petits groupes (pour qu'il n'y ait pas propagation).

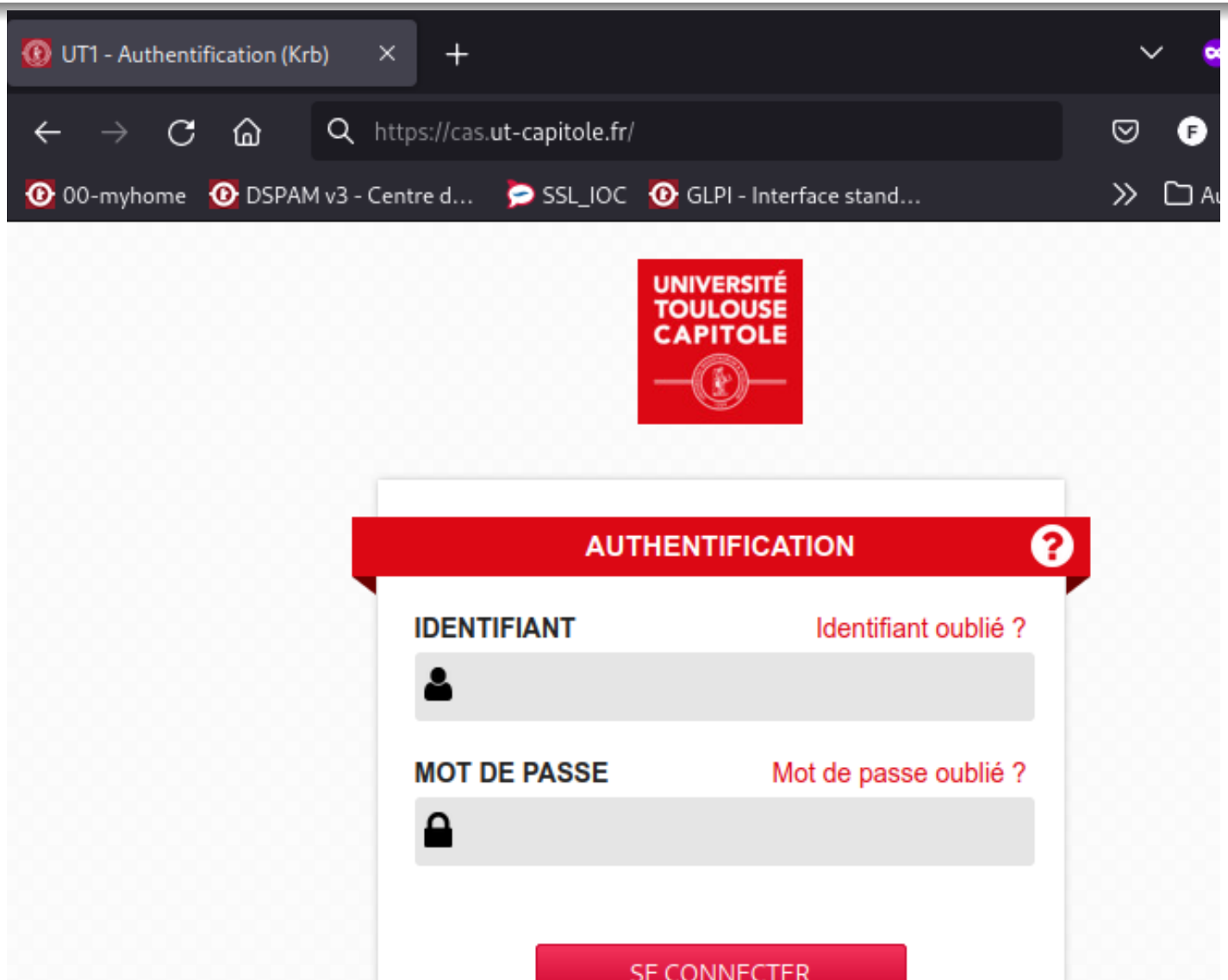
sans oublier les campagnes réelles, que vous devez reproduire.

Les campagnes qui font mal

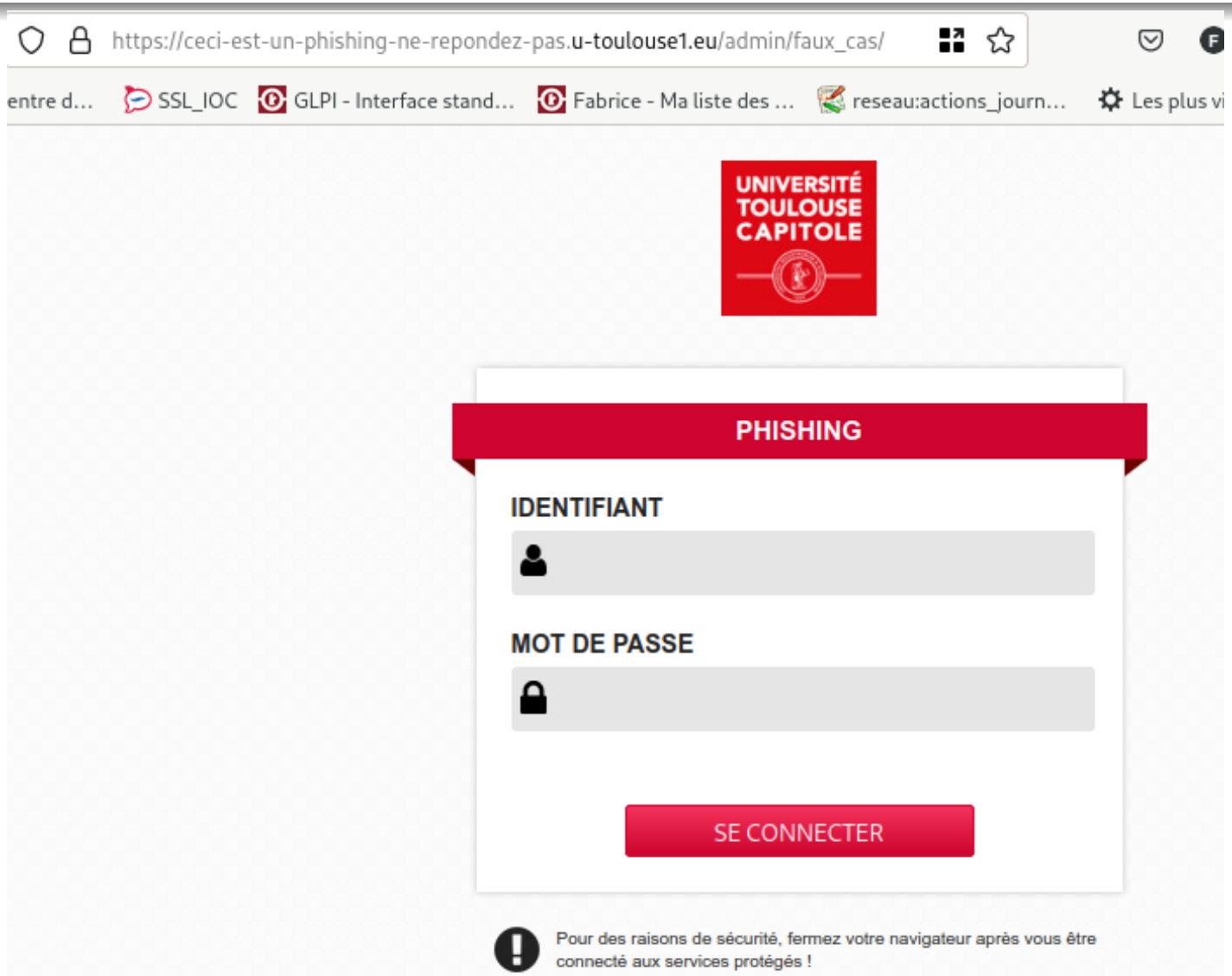
Certaines campagnes vont gêner les services

- L'argent et les congés
  - *"Pourquoi le contractuel a eu et pas moi ?"* (Incident remonté à la DRH)
- Les modes opérationnels
  - *"On a déjà du mal à leur faire comprendre la différence entre Intranet et Internet !"* (Service communication)
- Les extérieurs
  - *"Le ministère ne veut plus répondre à des enseignants pour rien"* (Mon HFD préféré)

Notre vraie mire d'authentification (CAS)



Laisser une chance aux utilisateurs



Laisser une chance aux utilisateurs.

Pour éviter

- les blacklistages par les utilisateurs avertis
- les frustrations *"On n'avait aucune chance"*
- quelques énervés.

C'est marqué dessus msieu.

Expliquer

- C'est tout le temps (une page web qui rappelle les bons principes, exemple : celui de l'UT Capitole)
- C'est avant (quand on envoie le mail d'avertissement)
- C'est après (quand ils se sont fait avoir)

Expliquer : soyez pédagogues

- Se faire avoir est une petite vexation, attention à ne pas tomber dans l'humiliation.
- Il est nécessaire de simplifier les consignes de détection :
  - la forme et l'url sont suffisantes dans notre environnement,
  - le mail ne fait même pas partie des critères de détection (mais ils comprennent seuls avec le temps, surtout si c'est pour détecter ce c.n de RSSI !).
- Il faut expliquer CLAIREMENT pourquoi elles ont été piégées.

Page d'explication

UNIVERSITÉ TOULOUSE CAPITOLE Vous venez de vous faire piéger

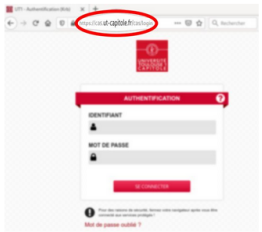
Vous venez de vous faire piéger, mais heureusement, ce n'est qu'un exercice (basé sur des phishings réels)

Vous avez fourni votre mot de passe à une page web qui n'est pas une page officielle de l'université Toulouse 1 Capitole

Que fallait-il regarder ?

L'adresse internet indiquée plus haut dans votre navigateur web est

- https://qqchose.**u-toulouse1.eu/**
- et non https://cas.**ut-capitole.fr** comme le montre l'image ci-dessous (cliquez dessus pour la voir en grand)



Un truc de plus ?

Quand vous avez entré votre mot de passe, les petits carrés habituels ne se sont pas affichés :

Quels risques avez-vous pris à titre personnel ?

Avec votre compte informatique, le pirate pourra prendre votre "identité numérique" et

- escroquer vos relations,
- leur envoyer des virus destructeurs de données,
- nuire à votre réputation.

Quels risques avez-vous fait prendre à l'UT1 ?

- Votre mot de passe permet à un pirate d'envoyer, en votre nom, plein de spams et de virus
- Par conséquent, l'UT1 serait considérée comme un "dangereux expéditeur de mails pourris",
- Par conséquent l'UT1 ne sera plus en mesure d'envoyer de mails pendant 24h vers gmail, hotmail et consort.
- De plus 2 à 5% des mails légitimes qui seront envoyés par l'UT1 pendant plusieurs semaines disparaitront sans avertissement.
- Enfin, le président de l'université sera sans doute obligé, dans le cadre du RGPD, d'avertir tous vos correspondants que leurs communications avec vous ont été diffusées.

Un conseil global

Il est acceptable de cliquer sur des liens dans les

UNIVERSITÉ TOULOUSE CAPITOLE

Plus le fait que vous passez pour un em...bêteur

Vous serez soupçonné d'être à l'origine de tous les phishings qu'ils reçoivent.

Et c'est pas bien ça ?

Beurk

Tu donnes envie.. un vrai bonheur

C'est vrai, mais en attendant

Les utilisateurs résistent et pas qu'au phishing !

Les bénéfices collatéraux

Les réflexes sont là : les utilisateurs résistent fortement, comparativement aux autres universités, aux

- Fraudes au président,
- Fraudes au loyer,
- Aux cryptolockeurs,
- Aux phishings "à titre personnel".

Les alternatives / évolutions

- GetGoPhish qui gère les campagnes avec des statistiques
- Les sociétés spécialisées ("Avant de cliquer", etc.)
  - gamification
  - augmentation de la résistance
  - plusieurs centaines de campagnes possibles.
  - obtention d'un "diplômes"
  - des vidéos (dont certaines viennent d'ailleurs de cybermalveillance
  - un prestataire extérieur c'est plus sérieux.
  - pour 20 000 étudiants et 2 000 personnels, c'était 50 000 € par an.
  - Top ten pour la direction.
- Envoyer des pièces jointes,
- Se mettre dans la peau du pirate.
- Simuler le phishing du support technique microsoft, avec un vrai numéro de téléphone... et un répondeur

Conclusion

- La pédagogie par la pratique marche :
  - Si vous avez un objectif clair (entrainer et non piéger),
  - Si le contexte est clair (explications, prévention, avertissement).
- Même si vous n'avez que 1 heure à y consacrer tous les 2 mois.
- Il ne faut faire aucun postulat sur les futures victimes, elles sont parfois TRES gradées.

Conclusion

Vous êtes dans la bonne voie si l'un de vos utilisateurs vous dit *Vous savez, j'ai expliqué à ma tata Jacotte qu'il ne fallait pas cliquer là parce que c'était un phishing. Comme quoi votre truc là, ça marche.*

En panne d'inspiration: ChatGPT