

*Plate-forme de cours sur l'administration systèmes et réseau pour les professionnels de l'informatique*

[IT-Connect](#) » [Cours - Tutoriels](#) » [Cybersécurité](#) » Sensibilisation des utilisateurs : création d'une campagne de phishing avec Gophish et Microsoft 365

**Création d'une campagne de phishing avec Gophish et Microsoft 365**

**Sensibilisation des utilisateurs**

IT-CONNECT

CYBERSÉCURITÉ

## Sensibilisation des utilisateurs : création d'une campagne de phishing avec Gophish et Microsoft 365



I. Présentation

II. Prérequis

III. Mise en place de Gophish

- A. Mise à jour et installation des dépendances
- B. Ouverture des ports
- C. Télécharger et installer Gophish
- D. Configurer Gophish et créer son service
- E. Configurer une base de données MariaDB pour Gophish

IV. Préparer la campagne de phishing

- A. Configurer le DNS de votre domaine avec Microsoft 365
- B. Configurer l'anti-phishing M365
- C. Configuration depuis l'interface Gophish
- D. Création de l'e-mail et de la page piège
- E. Création d'un groupe d'utilisateurs avec CSV
- F. Création et analyse de la campagne

V. Campagne de remédiation

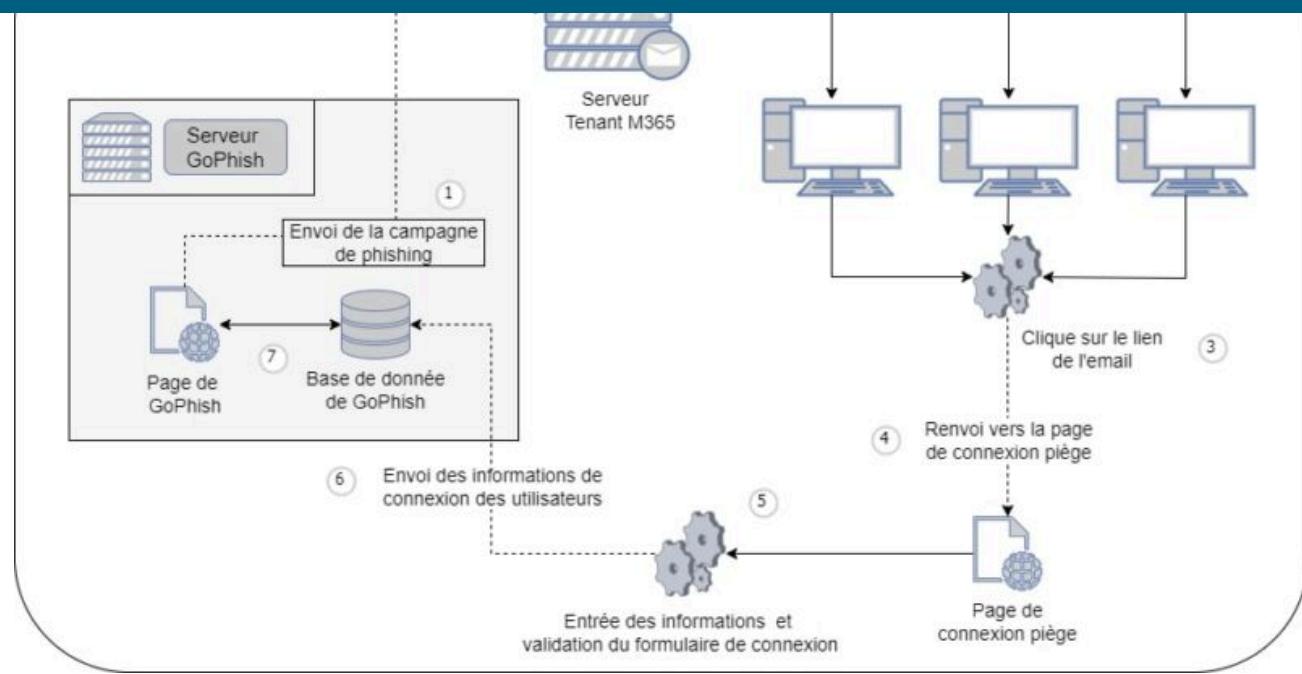
VI. Mettre à niveau votre version de Gophish

VII. Conclusion

## I. Présentation

Ce tutoriel explique comment déployer une campagne de phishing en utilisant Gophish et un tenant Microsoft 365 (M365). Vous apprendrez à configurer Gophish, à préparer votre domaine et à lancer des campagnes de phishing pour tester la vigilance de vos utilisateurs.

Il est destiné uniquement à **des fins éthiques et pédagogiques**. Les techniques décrites doivent être utilisées dans le cadre d'une **sensibilisation à la cybersécurité** ou d'une **évaluation des risques** pour **protéger** les utilisateurs. Toute utilisation malveillante de ces connaissances est **strictement interdite** et peut entraîner des **conséquences**.



**Gophish** est une plateforme open source conçue pour faciliter la création et la gestion de campagnes de phishing. Avec une interface utilisateur intuitive et de nombreuses fonctionnalités, Gophish permet de cibler facilement les utilisateurs et de suivre les résultats des campagnes en temps réel. Nous en avions parlé il y a quelques années dans [l'un de nos articles](#).

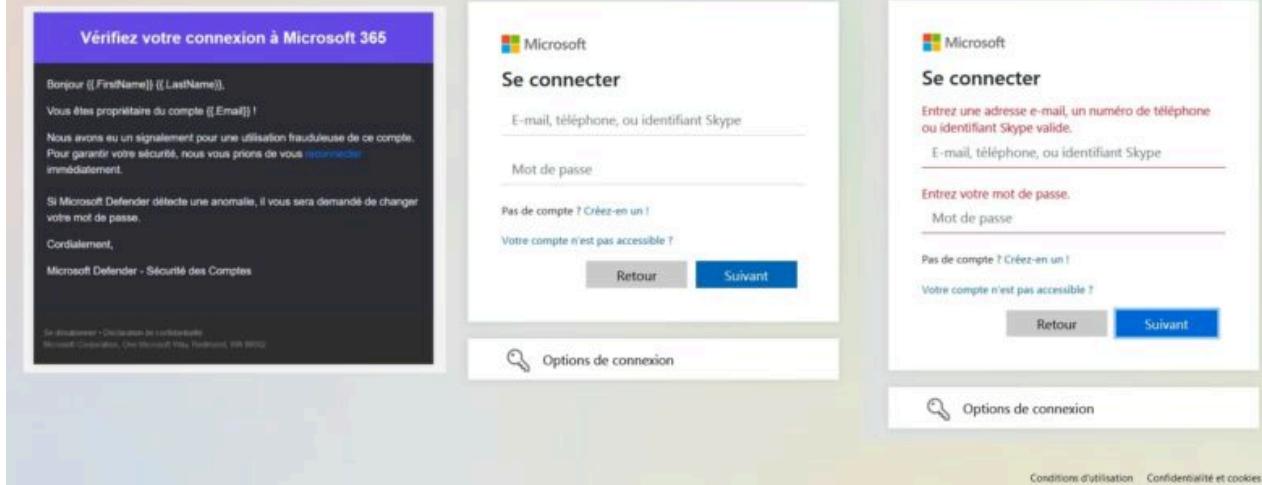
Il est possible de se passer de Gophish en utilisant **l'Attack Simulator** intégré à **Microsoft Defender**. Cependant, cette option nécessite une licence **Microsoft Defender for Office 365 Plan 2** qui a un coût et offre **moins de flexibilité** dans la gestion des campagnes d'hameçonnage.

- [Site officiel de Gophish](#)

## II. Prérequis

Avant de commencer, assurez-vous d'avoir les éléments suivants :

- Un domaine configuré chez votre fournisseur DNS (ce tutoriel utilise [kvrcybertechno.fr](#))
- Une **adresse IP publique** pour votre serveur
- Une licence **Microsoft Defender for Office 365 Plan 1** pour configurer la fonction de simulation d'hameçonnage sur Microsoft 365.
- Un e-mail et une page de destination à utiliser avec Gophish, ou utiliser [les pages du tutoriel](#), voir le visuel ci-après :



Pour l'exemple de ce tutoriel, le domaine utilisé sera "[kvrcybertechno.fr](http://kvrcybertechno.fr)" avec l'adresse IP publique "203.153.73.6". Ce domaine est très proche de l'original (en .com), ce qui le rend crédible pour les utilisateurs ciblés. Ceci rend notre campagne de phishing d'autant plus pertinente.

## III. Mise en place de Gophish

### A. Mise à jour et installation des dépendances

Commencez par mettre à jour votre système et installer les paquets nécessaires, tels que "`wget`" pour télécharger des fichiers et "`unzip`" pour extraire des archives.

```
# Debian
sudo apt -y update && sudo apt upgrade && sudo apt full-upgrade && sudo apt
autoclean && sudo apt clean
sudo apt -y install wget unzip

# AlmaLinux
sudo dnf update -y && sudo dnf upgrade -y && sudo dnf autoremove -y && sudo dnf
clean all
sudo dnf -y install wget unzip
```

### B. Ouverture des ports

Configurez le pare-feu de votre machine pour autoriser uniquement les flux nécessaires à la mise en œuvre du service Gophish. Le port 80 est utilisé pour le trafic HTTP, le port 443 pour le trafic HTTPS, et le port 3333 pour l'interface d'administration de Gophish.

```
# Debian
sudo apt install -y iptables
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```



```
sudo iptables-restore < /etc/iptables/rules.v4
sudo iptables -L -v -n

# AlmaLinux
sudo firewall-cmd --zone=public --add-port=80/tcp --permanent
sudo firewall-cmd --zone=public --add-port=443/tcp --permanent
sudo firewall-cmd --zone=public --add-port=3333/tcp --permanent
sudo firewall-cmd --reload
sudo firewall-cmd --list-all
```

Vous pourrez observer que les ports 80 (http), 443 (https) et 3333 (GoPhish) ont bien été ouverts :

```
pkts bytes target      prot opt in     out      source          destination
    0     0 ACCEPT      6   -- *       *        0.0.0.0/0        0.0.0.0/0          tcp dpt:80
    0     0 ACCEPT      6   -- *       *        0.0.0.0/0        0.0.0.0/0          tcp dpt:443
    0     0 ACCEPT      6   -- *       *        0.0.0.0/0        0.0.0.0/0          tcp dpt:3333

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out      source          destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out      source          destination
```

## C. Télécharger et installer Gophish

Téléchargez Gophish depuis [ce dépôt](#) pour une version française que j'ai recodée, apportant ainsi quelques améliorations, ou depuis [le dépôt officiel](#) pour une version anglaise :

```
# Version française (non officielle)
cd /tmp
wget
https://github.com/PassAndSecure/Template_Gophish/releases/download/gophish-
v0.12.1-linux-64bit-fr/gophish-v0.12.1-linux-64bit-fr.zip
ls -ll

# Version anglaise officielle
cd /tmp
wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-
v0.12.1-linux-64bit.zip
ls -ll
```

```
gophish-v0.12.1-linux-64bit 100%[=====] 31,69M 61,4MB/s   ds 0,5s
2024-08-04 22:38:28 (61,4 MB/s) - « gophish-v0.12.1-linux-64bit-fr.zip » sauvegardé [33232662/33232662]

total 32468
-rw-r--r-- 1 debuser debuser 33232662 4 août 22:19 gophish-v0.12.1-linux-64bit-fr.zip
drwx----- 3 root    root      4096 4 août 22:15 systemd-private-0579e7f55e9749bc943b6c30e76e2859-sys
logind.service-JCsRN1
drwx----- 3 root    root      4096 4 août 22:15 systemd-private-0579e7f55e9749bc943b6c30e76e2859-sys
timesyncd.service-mE4Vp2
drwx----- 2 root    root      4096 4 août 22:15 vmware-root_468-835298891
```

Une fois le téléchargement effectué, décompressez l'archive de Gophish dans le répertoire "/opt" pour une installation propre. Le répertoire "/opt" est couramment utilisé pour installer des



```
# Version française (non officielle)
sudo unzip gophish-v0.12.1-linux-64bit-fr.zip -d /opt
sudo mv /opt/gophish-v0.12.1-linux-64bit-fr /opt/gophish

# Version anglaise officielle
sudo unzip gophish-v0.12.1-linux-64bit.zip -d /opt
sudo mv /opt/gophish-v0.12.1-linux-64bit /opt/gophish
```

Puis rendez-le exécutable et lancez-le une première fois pour récupérer le mot de passe administrateur :

```
sudo chmod +x /opt/gophish/gophish
cd /opt/gophish
sudo ./gophish
```

**Explications :** la première commande rend le fichier Gophish exécutable. Les deux autres commandes naviguent dans le répertoire de Gophish et lancent l'application pour la première fois, ce qui génère le mot de passe administrateur.

Pour vous connecter, accédez à l'adresse IP publique ou privée avec le **port 3333**, selon les redirections que vous avez configurées en amont du tutoriel. Utilisez **admin** comme identifiant et le **mot de passe** récupéré précédemment. Pour ma part, ce sera : **192.168.1.17**.

**Il est possible que vous ne puissiez vous connecter avec la version officielle de Gophish, dans ce cas, il faudra faire un saut seulement sur la partie config.json avant de reprendre ici le tutoriel et de vous reconnecter.**

**Remarque :** un VPN interne à l'entreprise pourrait permettre aux utilisateurs d'accéder aux pages de Gophish si vous utilisez une adresse privée comme moi.

- [https://votre\\_adresse\\_ip:3333](https://votre_adresse_ip:3333)

Vous serez invité à changer le mot de passe. Je vous invite à autogénérer un mot de passe fort, par exemple, avec le site [generateur-motsdepass.fr](http://generateur-motsdepass.fr) ou l'application [KreatPass](#)).

## D. Configurer Gophish et créer son service

Supprimez le fichier de configuration actuel de Gophish et créez-en un nouveau :



Copiez ceci dans le fichier :

```
{  
    "admin_server": {  
        "listen_url": "0.0.0.0:3333",  
        "use_tls": true,  
        "cert_path": "gophish_admin.crt",  
        "key_path": "gophish_admin.key",  
        "trusted_origins": []  
    },  
    # Attention, supprimer tous ces commentaires, JSON ne les prend pas en  
charge  
    # Il est déconseillé d'utiliser TLS avec des certificats auto-signés comme  
ceux-ci  
    # Ils déclenchent la sécurité des navigateurs, ce qui alerte les  
utilisateurs  
    "phish_server": {  
        "#listen_url": "0.0.0.0:443",  
        "listen_url": "0.0.0.0:80",  
        "#use_tls": true,  
        "use_tls": false,  
        "cert_path": "gophish_admin.crt",  
        "key_path": "gophish_admin.key"  
    },  
    "db_name": "sqlite3",  
    "db_path": "gophish.db",  
    "migrations_prefix": "db/db_",  
    "contact_address": "",  
    "logging": {  
        "filename": "",  
        "level": ""  
    }  
}
```

Ce fichier de configuration définit les paramètres de Gophish, y compris les adresses et les ports sur lesquels les serveurs administratifs et de phishing vont écouter, les chemins des certificats TLS, et les paramètres de la base de données.

Quand votre configuration est créée, passez à la suite.

Créez un fichier de service pour lancer et arrêter Gophish, et pour le faire fonctionner même à l'arrêt de votre session :

```
sudo nano /etc/systemd/system/gophish.service
```



```
[Unit]
Description=Gophish Phishing Framework
After=network.target
[Service]
ExecStart=/opt/gophish/gophish
WorkingDirectory=/opt/gophish
User=root
Group=root
Restart=always
RestartSec=5
[Install]
WantedBy=multi-user.target
```

#### Explication des sections :

- **[Unit]** : Contient les métadonnées et les dépendances du service.
- **[Service]** : Définit comment le service doit être démarré et arrêté, ainsi que les paramètres d'exécution.
- **[Install]** : Spécifie comment le service doit être installé et démarré par défaut.

Redémarrez le démon, lancez Gophish, activez-le pour qu'il soit actif à chaque redémarrage et vérifiez son statut :

```
sudo systemctl daemon-reload
sudo systemctl restart gophish
sudo systemctl enable gophish
sudo systemctl status gophish
```

## E. Configurer une base de données MariaDB pour Gophish

Cette étape est facultative, mais recommandée. Gophish utilise par défaut une **base de données SQLite**, mais il est possible d'utiliser **MariaDB** pour une gestion plus robuste.

Pour installer MariaDB, vous pouvez utiliser la commande suivante :



```
# AlmaLinux
sudo dnf install -y mariadb-server
```

MariaDB est une alternative open source à MySQL, offrant des performances et une stabilité accrue.

Démarrez et activez MariaDB puis effectuez la sécurisation de base à l'aide du script "`mysql_secure_installation`" :

```
sudo systemctl start mariadb
sudo systemctl enable mariadb
sudo mysql_secure_installation
```

**Note** : pour les mots de passe lors de l'exécution de "`mysql_secure_installation`" et pour le futur utilisateur, évitez d'utiliser ces caractères suivants : %[];<>\_

Lors de l'exécution de "`mysql_secure_installation`", appuyez sur "y" à toutes les étapes sauf lorsque vous devez définir un mot de passe.

Ensuite, créez une nouvelle base de données et un nouvel utilisateur dédié pour cette base de données. Commencez par vous connecter à l'instance :

```
sudo mysql -u root -p
```

Puis, créez la base de données et l'utilisateur (adaptez les valeurs). Ici, la base de données s'appelle "`gophish`" et l'utilisateur dédié s'appelle "`gophish_user`".

```
CREATE DATABASE gophish CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'gophish_user'@'localhost' IDENTIFIED BY 'votre_mdp_fort';
GRANT ALL PRIVILEGES ON gophish.* TO 'gophish_user'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```



Changez le mode SQL pour supprimer "NO\_ZERO\_IN\_DATE" et "NO\_ZERO\_DATE" en créant un fichier de configuration pour MariaDB :

```
# Debian
echo -e
"\n[mysqld]\nsql_mode=ONLY_FULL_GROUP_BY,STRICT_TRANS_TABLES,ERROR_FOR_DIVISION_
BY_ZERO,NO_ENGINE_SUBSTITUTION" | sudo tee -a /etc/mysql/mariadb.conf.d/50-
server.cnf

sudo systemctl restart mariadb

# AlmaLinux
echo -e
"\n[mysqld]\nsql_mode=ONLY_FULL_GROUP_BY,STRICT_TRANS_TABLES,ERROR_FOR_DIVISION_
BY_ZERO,NO_ENGINE_SUBSTITUTION" | sudo tee -a /etc/my.cnf.d/mariadb-server.cnf

sudo systemctl restart mariadb
```

Explications :

- **echo -e "\n[mysqld]\nsql\_mode=..." :** cette commande ajoute de nouvelles directives au fichier de configuration de MariaDB pour définir le mode SQL à utiliser. Elle inclut des modes stricts pour garantir des comportements plus sûrs et prévisibles.
- **sudo tee -a /etc/mysql/mariadb.conf.d/50-server.cnf :** cette commande écrit les nouvelles directives dans le fichier de configuration du serveur MariaDB avec des droits sudo.

La base de données étant prête, vous devez modifier le fichier "config.json" de Gophish pour utiliser la nouvelle base de données :

```
sudo nano /opt/gophish/config.json
```

Changez "db\_name" et "db\_path" :



```
charset=utf8&parseTime=True&loc=UTC",
```

Voici des précisions pour vous aider :

- **gophish\_user** : l'utilisateur Gophish de votre base de données.
- **votre\_mdp\_fort** : le mot de passe de l'utilisateur Gophish.
- **gophish** : le nom de votre base de données Gophish.

Redémarrez le service Gophish :

```
sudo systemctl daemon-reload  
sudo systemctl restart gophish
```

Il ne vous reste plus qu'à récupérer le mot de passe, cette fois-ci dans les logs des journaux du service Gophish :

```
journalctl -u gophish.service | grep "password"
```

Voici de l'aide pour interpréter cette commande :

- **journalctl -u gophish.service** : cette commande affiche les logs pour le service *gophish.service*.
- **|** : l'opérateur pipeline redirige la sortie de la commande précédente (ici "*journalctl -u gophish.service*") comme entrée pour la commande suivante (ici "*grep*").
- **grep "password"** : cette commande recherche une chaîne de texte spécifique (ici, le mot *password*) dans l'entrée qui lui est fournie. Elle permet de filtrer les logs pour ne montrer que ceux qui contiennent ce mot clé.



Vous pourrez normalement accéder à la page de login, vous connecter avec le nouveau mot de passe qui vient d'être généré et changer le mot de passe.

## IV. Préparer la campagne de phishing

### A. Configurer le DNS de votre domaine avec Microsoft 365

Nous utiliserons un domaine OVHcloud, que nous allons configurer et relier à M365. Vous pouvez utiliser d'autres fournisseurs, cela ne pose aucun problème. Allez sur votre fournisseur et ajoutez un enregistrement "A" avec l'adresse IP publique de votre serveur Gophish. Vous pouvez voir votre adresse IP avec cette commande :

```
wget -qO- ifconfig.me
```

L'enregistrement pour OVHcloud se fait depuis [cette URL](#).

Sélectionnez votre domaine, puis ajoutez une entrée de type "A", laissez le domaine vide, ajoutez un **TTL personnalisé de 3600** et votre **adresse IP publique**. Pour cet exemple, c'est : **203.153.73.6** :



Le résultat final doit être comme suit :

Basculez sur l'interface d'administration de Microsoft 365. Vous pouvez maintenant aller sur votre tenant **M365 dans Domaines** pour ajouter votre domaine OVHcloud. Écrivez votre nom de domaine :



Choisissez d'ajouter un enregistrement "TXT" aux enregistrements DNS du domaine. Suivez les instructions et obtenez un résultat similaire :

Retournez sur M365, validez, puis sélectionnez : "Ajouter vos propres enregistrements DNS".

Laissez la case "**Exchange**" cochée, ajoutez vos propres enregistrements DNS, incluant les enregistrements **MX, CNAME, TXT et DKIM** dans les "**Options avancées**", validez et c'est terminé :

## B. Configurer l'anti-phishing M365

Pour autoriser une campagne de phishing interne, Microsoft a créé une sorte de "laissez-passer" que nous verrons après avoir [créé un utilisateur](#) qui servira de piégeur, avec votre nouveau domaine comme **Suffixe UPN**. A savoir que si la fonction de simulation n'est pas correctement configurée, les e-mails seront fréquemment classés comme spam par **Microsoft Defender** ou **Outlook**, dans environ 75% des cas.

Créez un compte "[no-reply-securite@votre-suffixe-upn](mailto:no-reply-securite@votre-suffixe-upn)", attribuez une licence (une simple licence **Exchange Online Plan 1** suffit) à ce compte, et [ajoutez une photo](#) pour plus de réalisme, en utilisant cette [image](#).



Configurez le domaine et l'IP dans la simulation d'hameçonnage de Defender :

- **Domaine** est le domaine qui va envoyer les e-mails, cela correspond au domaine du SMTP depuis lequel vous allez envoyer les e-mails et que vous avez configuré dans Gophish. **L'adresse IP** est l'adresse IP publique de votre serveur. À titre d'exemple, pour moi, c'est : **203.153.73.6** et **kvrcybertechno.fr**.

## C. Configuration depuis l'interface Gophish

Ayant dû arrêter Gophish précédemment pour activer son service, vous devrez vous reconnecter pour accéder à l'interface.

Une fois sur l'interface, allez dans "**Profils d'Envoi**" et ajoutez un nouveau profil avec cette configuration :

- **Nom** : SMTP Tenant Microsoft
- **Type d'interface** : SMTP
- **SMTP Depuis** : no-reply-securite@votre\_suffixe\_upn  
(utilisez le compte créé précédemment)
- **Hôte** : smtp.office365.com:587
- **Nom d'utilisateur** : no-reply-securite@votre\_suffixe\_upn
- **Mot de passe** : Le mot de passe fort de l'utilisateur
- **Cochez la case** : "Ignorer les erreurs de certificat" dans un premier temps

Cette configuration permet à Gophish d'utiliser les serveurs SMTP de Microsoft 365 pour envoyer des e-mails de phishing. En utilisant un compte créé spécifiquement pour cette tâche, vous assurez que les e-mails envoyés semblent légitimes.



## D. Création de l'e-mail et de la page piège

Sur l'interface de Gophish, allez dans "Modèles d'Email" et créez un nouveau modèle avec cette configuration :

- **Nom** : m365 Template
- **Expéditeur** : no-reply-securite@votre\_suffixe\_upn
- **Sujet** : No-reply alerte de sécurité Microsoft

Cliquez sur "**HTML**" et collez l'ensemble du code depuis mon [dépôt GitHub](#), puis sauvegardez.

**Remarque** : des arguments sont insérés exprès pour utiliser ou récupérer les informations des utilisateurs que nous créerons ultérieurement, par exemple : `{{{.Tracker}}}`.

En utilisant un modèle d'e-mail avec du HTML personnalisé, vous pouvez **créer des e-mails de phishing plus convaincants et professionnels**. Les arguments comme "`{{{.Tracker}}}`" permettent de suivre les interactions des utilisateurs avec l'e-mail.

Validez et obtenez ce résultat :

Allez dans "**Pages de Destination**", et créez un nouveau modèle avec cette configuration :

- **Nom** : m365 connexion
- **Cliquez sur HTML** : vous pouvez utiliser le modèle que j'ai codé [disponible ici](#), puis sauvegardez. J'ai inséré un argument "`{{{.Email}}}`" pour récupérer l'e-mail de l'utilisateur piégé, afin de donner un sentiment de confiance en arrivant sur la page.
- **Cochez** : "Capturer les données soumises" et "Capturer les mots de passe"
- **Collez cette URL** : dans "**Rediriger vers**" : <https://www.office.com/login?ru=%2f>  
(C'est l'URL de connexion Microsoft classique)

En configurant une page de destination qui capture les informations d'identification des utilisateurs et les redirige vers le site légitime de Microsoft, vous pouvez mesurer l'efficacité de votre campagne



Le résultat final sera comme ceci :

## E. Création d'un groupe d'utilisateurs avec CSV

Toujours sur l'interface de Gopish, accédez à "**Utilisateurs & Groupes**", et créez un nouveau groupe. Donnez le nom que vous voulez à ce groupe, par exemple "**Groupe-test-M365**". Vous aurez alors deux choix : soit créer des utilisateurs manuellement, soit importer un CSV.

J'ai scripté un PowerShell qui convertit un export utilisateur CSV depuis le centre d'administration Microsoft 365 en un CSV compatible avec Gophish. Il faudra télécharger les deux fichiers, vous les trouverez [ici](#).

C'est très simple d'utilisation. Il suffit de lancer le script, choisir votre CSV, puis dans la petite fenêtre qui s'ouvrira, donner un nom et valider. Le CSV converti apparaîtra dans le dossier d'origine du CSV initial.



L'importation d'utilisateurs via un CSV permet de gérer facilement de grands groupes de cibles pour vos campagnes de phishing. Le script PowerShell automatisé facilite la conversion des données exportées depuis M365 en un format compatible avec Gophish.

Il ne vous reste plus qu'à insérer le CSV dans Gophish et valider pour obtenir ce résultat :

## F. Création et analyse de la campagne

Dernière étape, rendez-vous dans "**Campagnes**", et créez-en une nouvelle avec cette configuration :

- **Nom** : Campagne-M365
- **Modèle d'E-mail** : Sélectionner m365 Template
- **Modèle de Page de Destination** : Sélectionner m365 Connexion
- **URL** : Utilisez l'URL avec votre IP, pour moi : <http://192.168.1.17>
- **Profils d'Envoi** : SMTP Tenant Microsoft
- **Groupes** : Groupe-test-M365

La configuration d'une campagne de phishing dans Gophish implique de sélectionner les modèles d'e-mail et de page de destination créés précédemment, de définir l'URL de phishing et d'associer la campagne à un groupe d'utilisateurs cibles. En utilisant le profil SMTP configuré, Gophish pourra envoyer les e-mails de phishing de manière crédible.

**Vous pouvez maintenant lancer la campagne !**

Pour le test, voici le résultat du courrier électronique envoyé par la campagne :



En cliquant sur "**vous reconnecter**", vous serez envoyé vers la page piège de connexion. Tous les autres liens sont des vrais que j'ai récupérés. Un peu d'HTML, de JavaScript et de Bootstrap m'ont permis de faire cette page. Plutôt réaliste, non ?



En cliquant sur suivant, vous enverrez, d'une part, les identifiants vers Gophish, et d'autre part, serez redirigé vers la vraie page de connexion. Le côté traître est que si vous avez déjà des cookies de connexion enregistrés, vous serez envoyé vers votre page Microsoft en ayant vraiment l'impression de vous être connecté à l'instant avec cette page piège.

Il ne vous reste plus qu'à retourner sur Gophish et observer les résultats. 😊



## V. Campagne de remédiation

Maintenant que votre campagne a porté ses fruits, je vous conseille de sensibiliser les utilisateurs impactés avec une **campagne de remédiation**.

Tout d'abord, sur M365, **créez un nouvel utilisateur** qui servira de **communicant officiel et légitime auprès de vos utilisateurs**. Associez le logo de votre entreprise **en photo** de profil de ce compte pour le rendre plus officiel le compte.

Sur Gophish, créez un **nouveau profil d'envoi** pour cet utilisateur avec des paramètres similaires au piège, **sauf l'e-mail** bien sûr.

De la même manière que précédemment, **créez un template d'E-mail**. Vous pouvez utiliser **ce template** à finir de compléter avec vos informations. Il dispose, en plus des autres, d'un argument "`{{{.TrackingURL}}}`" pour savoir qui a bien ouvert l'e-mail. Vous pouvez voir ci-dessous un exemple du template complété :



Il est possible que le **tracking** ne fonctionne pas, car certaines **boîtes e-mail bloquent l'image de tracking** de Gophish. Pour contourner en partie le problème, vous pouvez remplacer l'**URL de votre solution de ticketing** par l'argument "`{{.URL}}`" et créer une **page piège** qui pointe vers l'**URL de votre solution de ticketing**. Comme ça, lorsque vos **utilisateurs cliqueront sur le lien**, ils seront envoyés vers la **page piège** qui les renverra vers votre **page de ticketing** (via une redirection). Ainsi, vous verrez des **événements de clic** dans le **rappor**t Gophish.



```
<!DOCTYPE html>
<html lang="fr">
<head>
<meta charset="UTF-8">
<meta http-equiv="refresh"
content="0;url=https://votre_domaine/solution_de_ticket.html">
<title>Redirection</title>
</head>
<body>
<p>Si vous n'êtes pas redirigé automatiquement, <a href="https://votre_domaine/solution_de_ticket.html">cliquez ici</a>.</p>
</body>
</html>
```

Il ne vous reste plus qu'à **commencer une nouvelle campagne** avec ces nouvelles pages.

## VI. Mettre à niveau votre version de Gophish

**Terminons avec une astuce** : si vous voulez passer de la version Anglaise à Française ou inversement, il suffirait simplement de lancer l'un de ces scripts. Ils ont pour fonction de télécharger la version alternative à la vôtre, supprimer les fichiers dans "**templates**", "**static**", et de les remplacer par ceux de l'alternative. Ça ne changera rien aux informations stockées dans la base de données, donc c'est sans risque pour vous, et bien sûr, il ne restera aucun fichier résiduel.

- **Passage de la version Française à Anglaise**

```
cd /tmp
wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-
v0.12.1-linux-64bit.zip
mkdir -p /tmp/gophish_unpack
sudo unzip gophish-v0.12.1-linux-64bit.zip -d /tmp/gophish_unpack
sudo mv /tmp/gophish_unpack /tmp/gophish
sudo rm -rf /opt/gophish/templates/*
sudo rm -rf /opt/gophish/static/*
sudo cp -r /tmp/gophish/templates/* /opt/gophish/templates
sudo cp -r /tmp/gophish/static/* /opt/gophish/static
sudo rm -rf gophish-v0.12.1-linux-64bit.zip
sudo rm -rf gophish
```

- **Passage de la version Anglaise à Française**

```
cd /tmp
wget
https://github.com/PassAndSecure/Template_Gophish/releases/download/gophish-
```



```
sudo mv /tmp/gophish_unpack /tmp/gophish
sudo rm -rf /opt/gophish/templates/*
sudo rm -rf /opt/gophish/static/*
sudo cp -r /tmp/gophish/gophish-v0.12.1-linux-64bit-fr/templates/*
/opt/gophish/templates
sudo cp -r /tmp/gophish/gophish-v0.12.1-linux-64bit-fr/static/*
/opt/gophish/static
sudo rm -rf gophish-v0.12.1-linux-64bit-fr.zip
sudo rm -rf gophish
```

Ceci vous facilitera la tâche si vous décidez de changer de version.

## VII. Conclusion

En suivant ce tutoriel, vous avez appris à **déployer une campagne de phishing** en utilisant **Gophish** et un **tenant Microsoft 365 (M365)** pour tester la vigilance de vos utilisateurs !

L'intégration de cet outil dans votre **stratégie de cybersécurité** est une étape essentielle pour renforcer la **sensibilisation** de vos collaborateurs et identifier les **vulnérabilités humaines**.

Si vous rencontrez des difficultés dans la mise en œuvre de ce processus ou avez des questions, n'hésitez pas à laisser un commentaire sur cet article. Pour aller plus loin, consultez cet article :

- [Déployer un reverse proxy Nginx et un certificat Let's Encrypt pour Gophish](#)

**Killian VAN RUYMBEKE** | Ingénieur Cybersécurité M1

Ingénieur Cybersécurité M1 en alternance, j'ai une forte appétence pour tous les domaines technologiques. Dans un esprit d'entraide, j'essaie de partager les connaissances que j'ai pu acquérir à travers mes articles.

[See Full Bio >](#)



AINTENANT !

BON PLAN DE L'AUTOMNE 2024 : JUS  
QU'À 57 EUROS DE REMISE SUR LES  
SERRURES CONNECTÉES WELOCK !

## ↳ Vous pourrez aussi aimer



Recherchez tous les comptes correspondants à un pseudo avec Sherlock

28/12/2021 4

Gérez les vulnérabilités et mettez en conformité vos machines avec NX

07/06/2023 5

## 1 commentaire sur “Sensibilisation des utilisateurs : création d'une campagne de phishing avec Gophish et Microsoft 365”



DUNEUF

24/09/2024 à 11:33 Permalink

Merci pour ton travail, ça aide pas mal dans notre métier

[Répondre](#)



Votre adresse e-mail ne sera pas publiée. Les champs obligatoires sont indiqués avec \*

**Commentaire \***

**Nom \***

**E-mail \***

**Site web**



Enregistrer mon nom, mon e-mail et mon site dans le navigateur pour mon prochain commentaire.

**Laisser un commentaire**

**Newsletter : 1 e-mail par semaine !**

Votre adresse e-mail\*



A la une

A large thumbnail for an article titled "Script Bash". The title is in large yellow letters with a penguin icon next to it. Below the title is the subtitle "Générer des nombres aléatoires". There is an illustration of a box with question marks above it and a grid of numbers (5, 4, 2, 1, 8, 9, 6, 3) floating nearby. The background is dark with some light effects.

BASH

LINUX

## Script Bash – Comment générer des nombres aléatoires sous Linux ?

30/09/2024 Mickael Dorigny 0 commentaire



Windows – Exécuter un script PowerShell en tant que tâche planifiée immédiate avec une GPO

30/09/2024 0 commentaire



Perplexity.ai : le moteur de recherche boosté à l'intelligence artificielle

29/09/2024 0 commentaire



Stirling PDF : comment ajouter une signature numérique à un PDF ?

28/09/2024 1 commentaire



Windows 11 : Recall peut être désinstallé et il est plus sécurisé !

27/09/2024 0 commentaire



Windows 11 KB5043145 : que contient cette mise à jour ? Il ne s'agit pas de Windows 11 24H2 !

27/09/2024 2 commentaires

## Nos derniers cours gratuits

# Maîtrisez Cisco IOS Les bases indispensables



Maîtrisez Cisco IOS : les bases indispensables



Florian Duchemin

# Débuter avec Hyper-V

## La virtualisation sur Windows Server



Windows Server



IT-CONNECT

COURS EN LIGNE

26 chapitres



Débuter avec Hyper-V – La virtualisation sur Windows Server 2022



Florian BURNEL

Vous cherchez quelque chose ?

Recherche



Découvrir IT-Connect



Comment contribuer sur IT-Connect ?

Contact

Espace annonceurs

L'Équipe

Offres d'emploi

Politique de confidentialité

Puis-je réutiliser le contenu publié sur IT-Connect ?

Soutenir IT-Connect

Espace personnel

Inscription

Connexion

Flux des publications

Recommandations

Blogmotion

Délibérata

Tech2tech

Générateur de mots de passe

