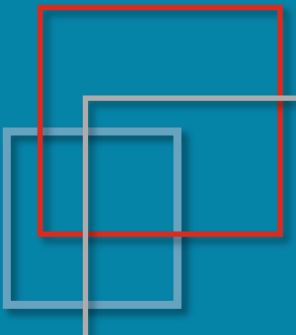


B2-5

アタックサーフェスのその先にあるもの ～ リアルな攻撃、リアルな現状



自己紹介

関根 章弘



- 1995年頃 インターネット接続ブーム時に構築支援を行う要件を満たすために必要に迫られてsendmail.cfをカスタマイズ
- 2000年頃 商用サービス向けの大規模メールシステムの構築に関わる
- 海外のメール製品ベンダに所属し日本のサービスに導入
- 2003年 迷惑メール対策カンファレンスの運営に携わる
- 2019年 Vade Japanに入社、顧客サポートを担当

自己会社紹介

- Vade Japan株式会社（本社はフランス共和国 リール）
- AIエンジンを用いた予測的メール防衛の世界的リーダー
- 全世界で14億を超えるメールボックスを保護
- 日本国内にメール脅威の分析を行う技術チームを保有

本社オフィス外観



侵入経路として狙われるEmail

- サイバー犯罪の多くは簡単なメールで始まる
 - メールは主な通信手段であるがゆえに、サイバー脅威の最大の媒体にもなっています。フィッシングは最も一般的かつ効果的な攻撃手法です。また、ビジネスメール詐欺(BEC)としても知られるスパフィッシングは大きな被害をもたらします。2022年に報告された被害額として27億ドル(USD)にもなります。
- 2023年第3四半期に攻撃の大幅な増加を検出
 - フィッシング数量は前四半期と比較して173%増加、マルウェアも110%増加と、いずれも2倍以上に急増加しました。
- Microsoft, Googleのプロダクティビティソフトウェアが最大の標的
 - プロダクティビティスイートは、フィッシング犯にとって魅力的な標的です。一連の統合アプリケーションは、フィッシング犯にユーザーを悪用できる機会を増やします。
 - 個人を狙ったフィッシングはFacebookがトップブランド

フィッシングのターゲット

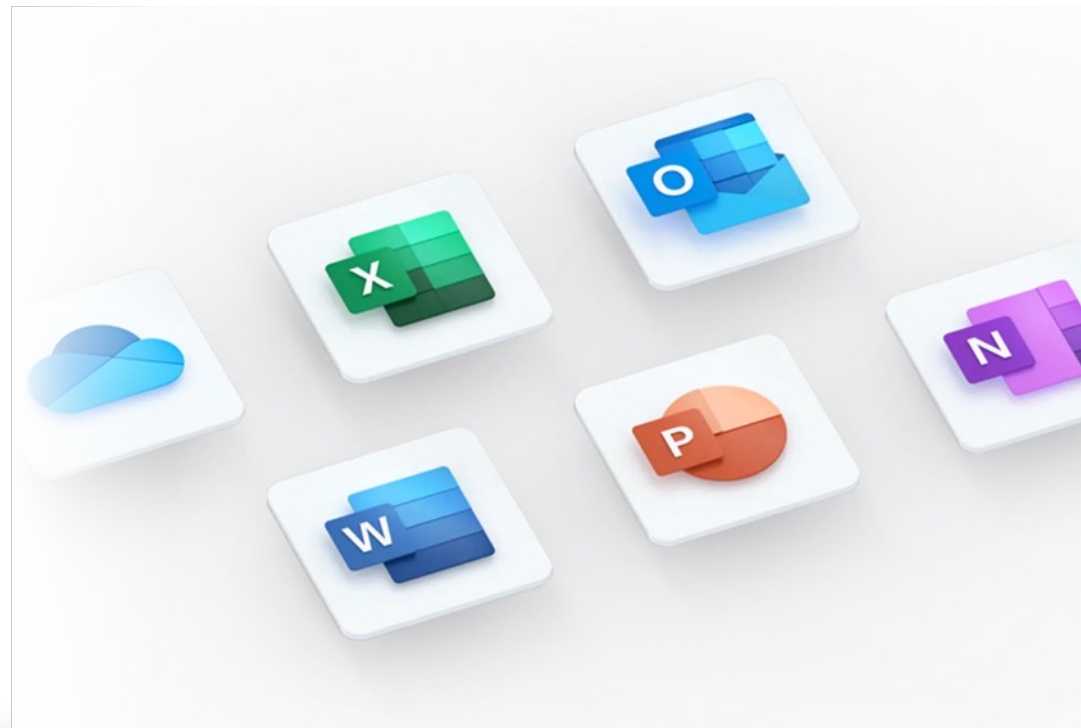
Phishers' Favorites 2022 20 MOST IMPERSONATED BRANDS

Number	Movement	Brand	Category	Unique Phishing URLs
1	0	Facebook	Social Media	25551
2	0	Microsoft	Cloud	22531
3	↑ 25	Google	Cloud	19695
4	↑ 6	PayPal	Financial Services	15863
5	↑ 13	MTB	Financial Services	13330
6	0	Orange	Internet/Telco	12839
7	↓ -4	Crédit Agricole	Financial Services	11998
8	↓ -4	WhatsApp	Social Media	10388
9	↓ -4	La Banque Postale	Financial Services	10242
10	N/A	au	Internet/Telco	9542
11	↑ 1	Netflix	Cloud	9018
12	↑ 7	Apple	E-Commerce/Logistics	7634
13	↓ -6	Amazon	E-Commerce/Logistics	7364
14	↓ -1	Wells Fargo	Financial Services	6885
15	↓ -7	Chase	Financial Services	6788
16	↑ 6	Instagram	Social Media	6403
17	↓ -8	Comcast	Internet/Telco	6327
18	↓ -4	Rakuten	E-Commerce/Logistics	4850
19	↑ 52	Credit Saison	Financial Services	4593
20	↓ -5	Adobe	Cloud	4503

M365のクレデンシャルを狙うフィッシング

Microsoft 365はフィッシング
攻撃の最大の標的

ひとつのアカウントに侵入すれば、
攻撃者はBECに利用可能な
ツールを多く手に入れることが
できる



Microsoft 365



2億5800万
ユーザー



100万顧客



メール市場の
90%を占有

M365のクレデンシャルを狙うフィッシング

Important : credentials update



o Vade Support <IT-request@office36o.com>

2022年9月9日 金曜日 23:15

宛先: ❌ akihiro.sekine@vadesecure.com

⚠️ プライバシー保護のため、このメッセージの一部の外部画像はダウンロードされま… [設定に移動](#) [外部画像のダウンロード](#)



Important : credentials update

The IT department wishes to strenghten the security of internet and intranet accesses by imposing the update of the passwords of each user according to the following strong password policy :

At least 12 characters long
Includes lower case and upper case characters, numbers and special characters
Is not a word preceded of followed by a number

[I update my password now](#)



Microsoft Password - Action Alert vadesecure.com



o IT Corporation <kirkridge@kirkridge.org>

2022年10月24日 月曜日 23:41

宛先: ❌ akihiro.sekine@vadesecure.com

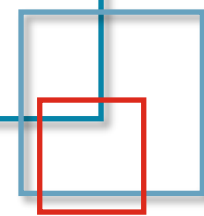
! このメッセージの重要度は "高" です。



Hello akihiro.sekine@vadesecure.com, your password expires today.

Keep Same Password

Vadesecure.com

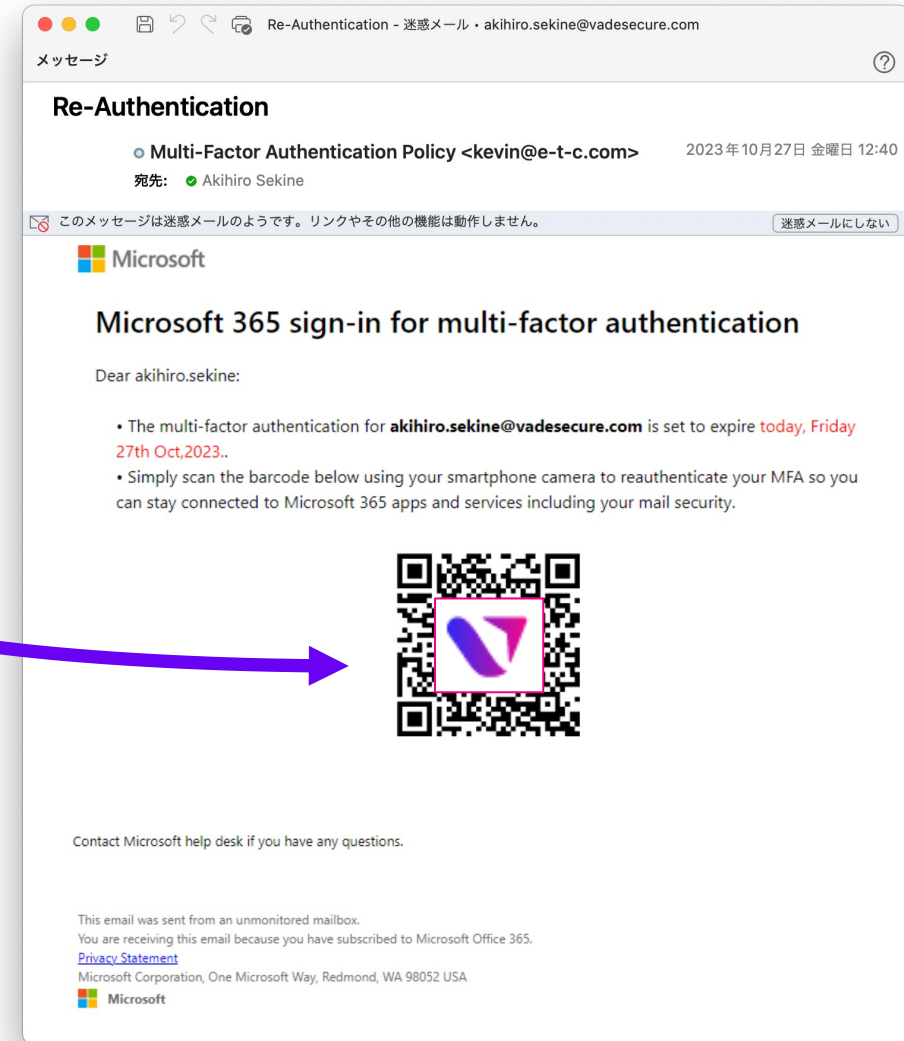


M365 QRishing攻撃

- MFAを再有効化しなければならないことをユーザーに警告するフィッシングメール
- QRコードを使用してフィッシングサイトに誘導する

M365 QRishing攻撃

- MFAを再有効化しなければならないことをユーザーに警告するフィッシングメール
- QRコードを使用してフィッシングサイトに誘導する



M365 QRishing攻撃

- メッセージも含めて1枚の画像のみの構成



- URLはQRに埋め込まれているため直接チェックすることができません
- 画像の一部を変えるだけで容易にハッシュ値を変えられるため、攻撃者は膨大なパターンを生成できます

Re-Authentication



Multi-Factor Authentication Policy <kevin@e-t-c.com>

2023年10月27日 金曜日 12:40

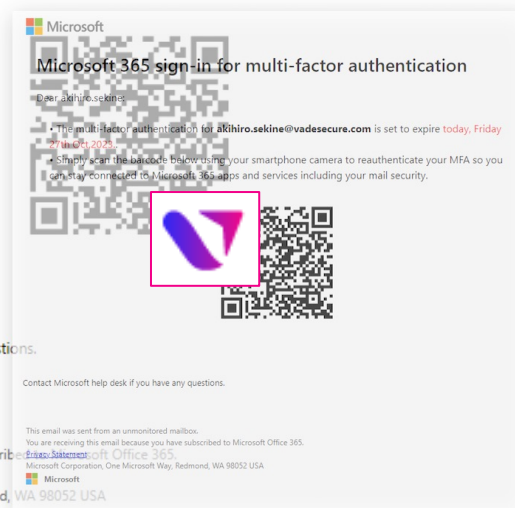
宛先: akihiro.sekine@vadesecure.com



Microsoft 365 sign-in for multi-factor authentication

Dear akihiro.sekine:

- The multi-factor authentication for **akihiro.sekine@vadesecure.com** is set to expire **today, Friday 27th Oct, 2023.**
- Simply scan the barcode below using your smartphone camera to reauthenticate your MFA so you can stay connected to Microsoft 365 apps and services including your mail security.



Contact Microsoft help desk if you have any questions.

Contact Microsoft help desk if you have any questions.

This email was sent from an unmonitored mailbox.

You are receiving this email because you have subscribed to this email.

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA



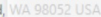
This email was sent from an unmonitored mailbox.

You are receiving this email because you have subscribed to this email.

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA

Microsoft



フィッシングURL、ドメイン

URL: <https://adidosports.com/assets/js/index.html#...>

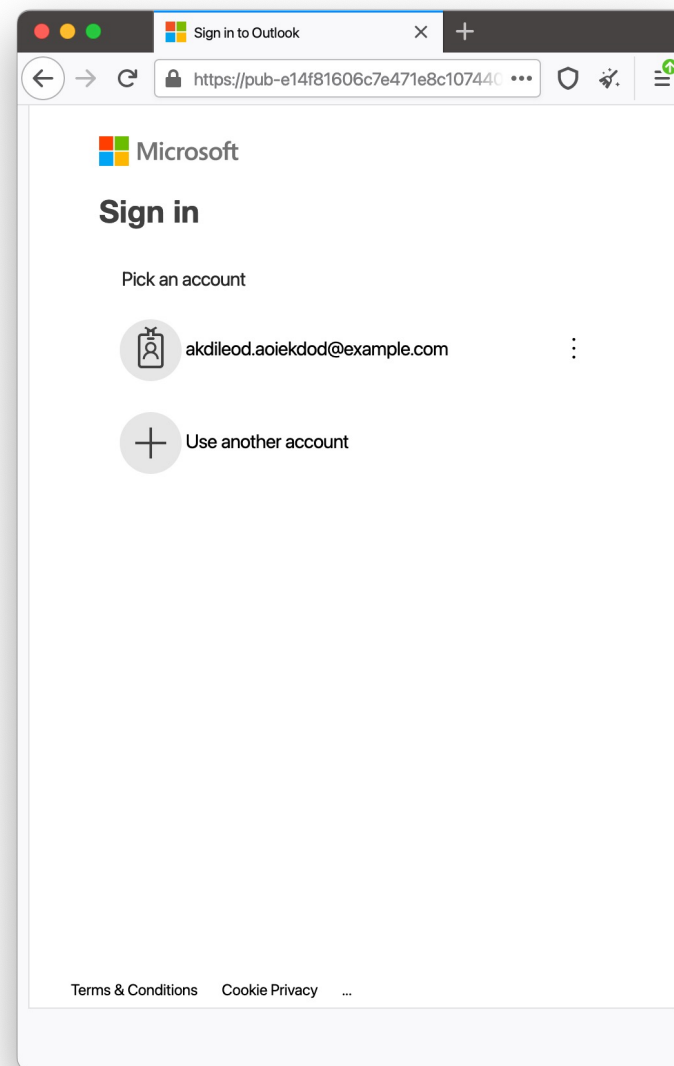
whois Domain Name: ADIDOSPORTS.COM
Registry Domain ID: 2800557986_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2023-09-23T08:05:10Z
Creation Date: 2023-07-24T13:41:26Z

Vade内の統計情報には2022/07に利用された痕跡が残っていました

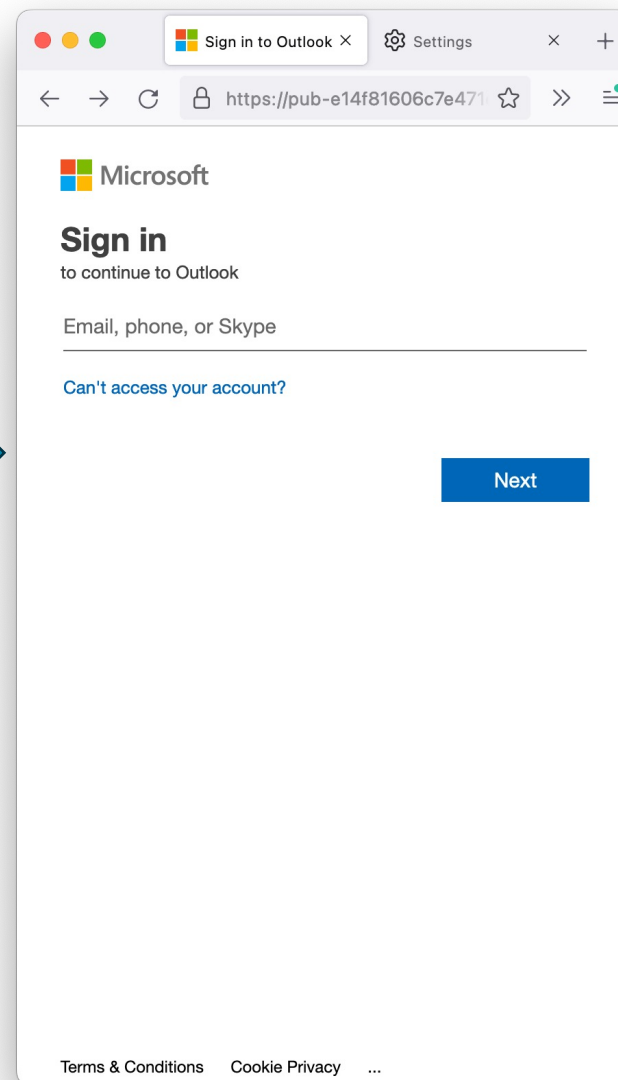
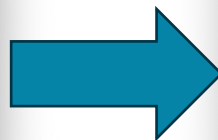
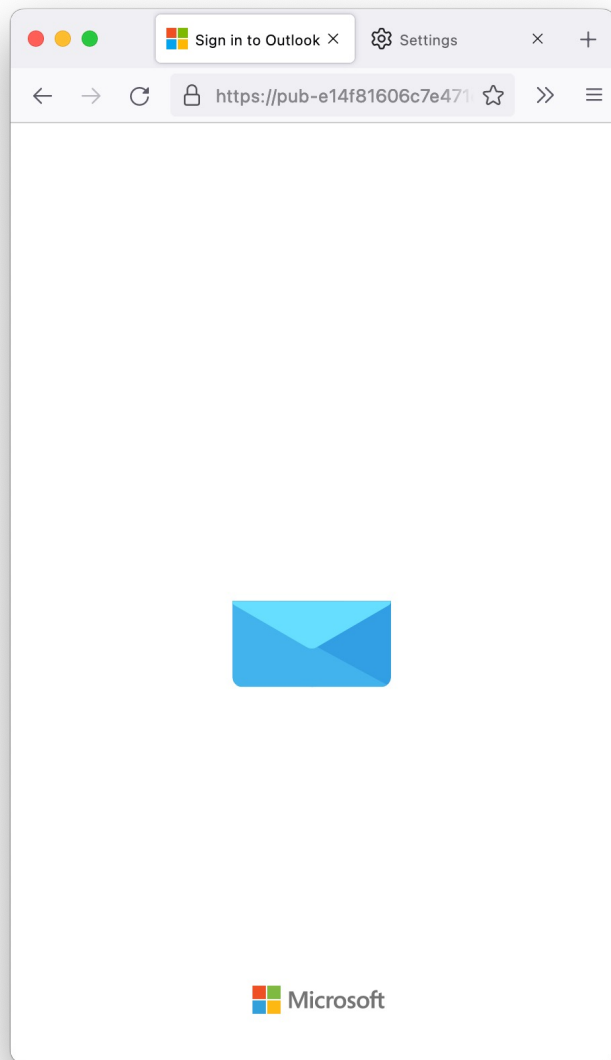
M365 QRishingサイト

アクセス結果

- Cloudflareを利用
- 認証画面を表示する前に、スプラッシュ画面を経由することで正当な雰囲気を作り出します

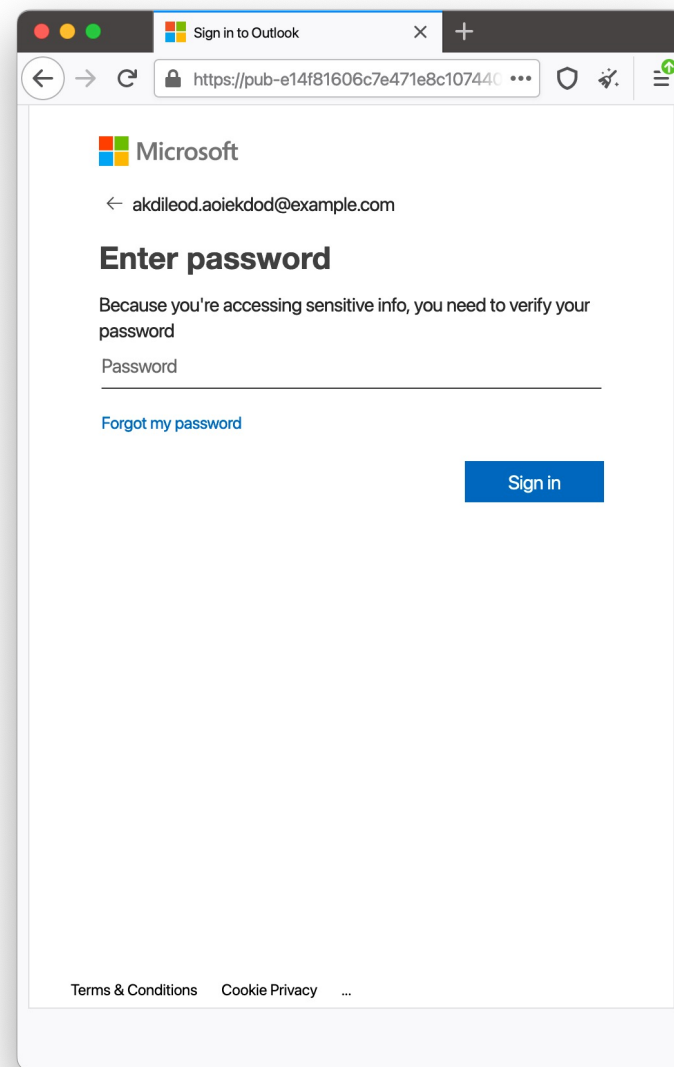


M365 QRishingサイト



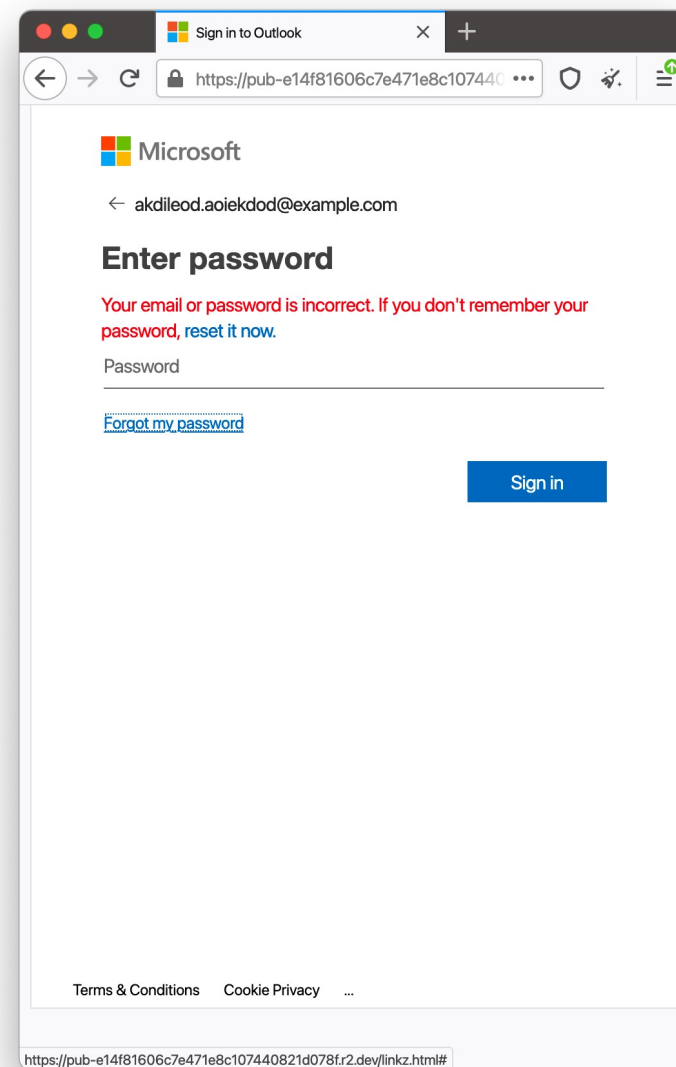
M365 QRishingサイト

- アカウントを選択するとパスワードを要求します。



M365 QRishingサイト

- 認証エラーとなりパスワードリセットに進むところですが、機能しませんでした。
- フッター部分にある“Terms & Conditions”と“Cookie Privacy”のリンクは本家のページにリンクされています。



URL難読化テクニック

- フィルターを回避するためにURLを難読化するテクニックが次々と開発されています。QRコードの利用もその一つです。
- その他の難読化テクニックも用いた例
 1. aHR0cHM6Ly95dHh6bWFXLmNvbS8=
 2. <https://YTXZMAQ.COM/>

URL難読化テクニック

1. aHR0cHM6Ly95dHh6bWFXLmNvbS8=

- BASE64エンコード
<https://ytxzmaq.com/>

2. <https://YTXZMAQ.COM/>

- UTF-8、囲み英数字補助

囲み英数字補助

Enclosed Alphanumeric Supplement

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
F09F8480	0.	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,					
F09F8490	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)
F09F84A0	(Q)	(R)	(S)	(T)	(U)	(V)	(W)	(X)	(Y)	(Z)						
F09F84B0																
F09F8580																
F09F8590																
F09F85A0																

Thank you

