Issue 34 10 Nov 2023

Weekly Scams Bulletin

A publication by the Singapore Police Force and the National Crime Prevention Council

Trending Scams in the past week:

Fake Friend Call Scam

Job Scam

Investment Scam

E-Commerce Scam (Variants)

Phishing Scam

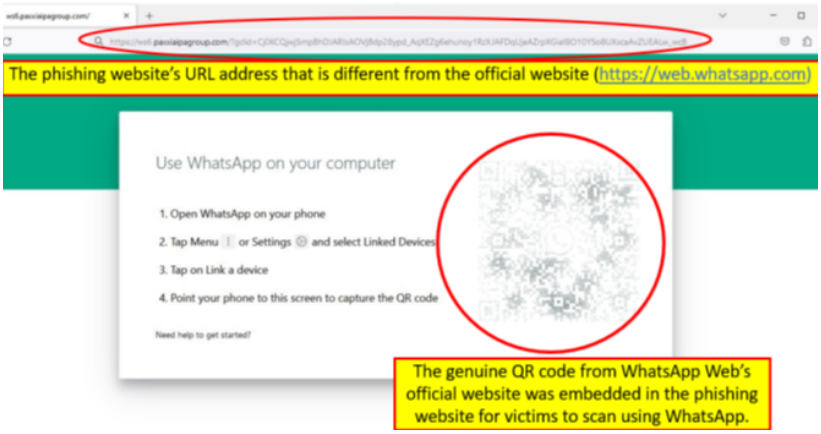
Using WhatsApp Web? There's a new phishing scam type that can compromise your WhatsApp account.

Scam Tactics

To access WhatsApp on their computer/tablet, victims search for "WhatsApp web" version, click on the first few search engine results, without verifying the URL. Setup by scammers, these URLs replicate the interface of WhatsApp web and contain a QR code.

Victims would scan the QR code and authorise WhatsApp access on their computer/tablet, but the phishing site would be unresponsive. Instead, scammers would gain concurrent access to victims' WhatsApp account, without their knowledge. Scammers would reach out to victims' contacts to ask for unusual requests such as asking for loans/money transfers or i-banking/personal details.

Victims would realise their WhatsApp accounts were compromised after their contacts notify them of the unusual requests received.



Screenshot of the phishing website impersonating the official WhatsApp Web

Some Precautionary Measures:

ADD – Security features to your WhatsApp account by enabling the 'Two-Step Verification' feature. This can be done on WhatsApp's in-app Settings. Set a device code and be aware of who has physical access to your phone.

CHECK – That you are on WhatsApp Web's official website. Be wary of unusual requests received over WhatsApp, even if they were sent by your WhatsApp contacts.

Check your linked devices regularly. Go to WhatsApp Settings > Linked Devices to review all devices linked to your account. To remove a linked device, tap the device > Log Out.

TELL – authorities, family, and friends about scams. Never share your WhatsApp account verification codes, personal information, banking details and OTPs with anyone; report any fraudulent transactions to your bank immediately.

For more information on this scam, visit SPF | News (police.gov.sg)

34号刊 2023年11月10日

诈骗周报

新加坡警察部队和全国罪案防范理事会刊物

过去一周
诈骗趋势:

假朋友来电骗局

求职诈骗

投资诈骗

电子商务骗局
(各种手法)

钓鱼骗局

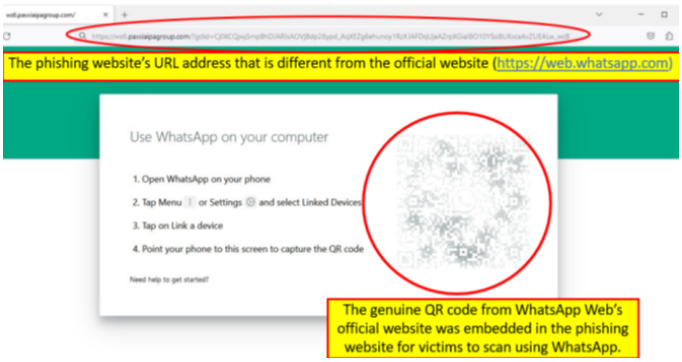
使用网页版WhatsApp 吗?
新钓鱼诈骗手法能侵入您的WhatsApp账户。

诈骗手法

为了在电脑/平板电脑使用WhatsApp,受害者会在搜索引擎寻找网页版WhatsApp并在没核实网址的情况下，点击搜索结果的首几个链接。

受害者扫描二维码并授权WhatsApp访问他们的电脑/平板电脑后，会发现钓鱼网页没有反应。相反的，骗子在受害者不知情的情况下，能同时访问受害者的WhatsApp 账户。

骗子会向受害者的联络人发出不寻常请求，例如借款/转账或索取网上银行/个人资料。受害者会在接到联络人关于不寻常请求的通知后，才意识到自己的WhatsApp账户被盗用了。



【截图：假冒官方网页版WhatsApp的钓鱼网站】

一些预防措施:

添加 – 在您的WhatsApp应用程序设置添加账户"双重认证"安全功能。为您的设备设置密码并留意能接触您手机的人。

查证 – 确保您访问的是网页版 WhatsApp官方网站。即便发送人是您的联系人，也务必提防来自 WhatsApp 的不寻常请求。

定期检查您的绑定设备。到 WhatsApp 设置>已绑定设备检查所有与您账户绑定的设备。若想删除绑定设备，请选该设备>登出即可。

通报 – 当局、家人和朋友诈骗案件趋势。切勿与他人分享您 WhatsApp 账户认证密码、个人资料、银行资料及一次性密码（OTP)。立即向银行举报任何欺诈性的交易。

欲了解更多关于这个骗局的信息，请浏览 SPF | News (police.gov.sg)

Isu no. 34 10 Nov 2023

Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN SEPANJANG MINGGU LEPAS:

Penipuan Panggilan Kawan Palsu

Penipuan Pekerjaan

Penipuan Pelaburan

Penipuan E-Dagang (Varian penipuan)

Penipuan Pancingan Data

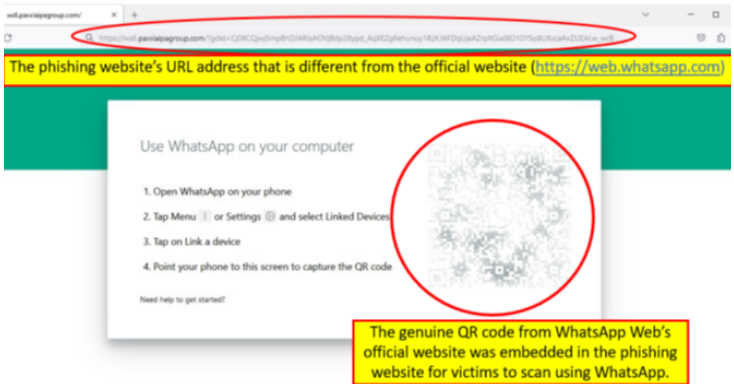
Gunakan Aplikasi WhatsApp Web? Terdapat sejenis penipuan pancingan data baru yang boleh menjejaskan akaun WhatsApp anda.

Taktik Penipuan

Untuk mengakses akaun WhatsApp mereka daripada komputer/tablet, mangsa mencari versi laman "WhatsApp web", dan kemudian klik pada beberapa hasil enjin carian pertama yang keluar, tanpa mengesahkan URL tersebut. URL ini direka oleh penipu dan ia meniru antara muka web WhatsApp dan mengandungi kod QR.

Mangsa akan mengimbas kod QR tersebut untuk memberi izin kepada WhatsApp Web untuk membolehkan mereka mengakses akaun WhatsApp dari komputer/tablet mereka, tetapi laman web pancingan data tersebut akan menjadi tidak responsif. Sebaliknya, penipu akan mendapat akses serentak ke akaun WhatsApp mangsa, tanpa pengetahuan mereka. Penipu akan menghubungi kenalan mangsa dan membuat permintaan yang mencurigakan seperti meminta pinjaman/ pemindahan wang atau butiran perbankan internet/maklumat peribadi.

Mangsa akan menyedari akaun WhatsApp mereka telah dikompromi selepas kenalan mereka memberitahu mereka tentang permintaan yang mencurigakan yang mereka terima.



[Tangkap layar laman web pancingan data yang menyamar sebagai laman rasmi WhatsApp Web]

Beberapa langkah berjaga-jaga:

MASUKKAN – Ciri-ciri keselamatan pada akaun WhatsApp anda dengan membolehkan ciri 'Pengesahan Dua Langkah'. Ini boleh dilakukan di tetapan dalam aplikasi WhatsApp. Tetapkan sebuah kod peranti dan berhati-hati terhadap sesiapa yang boleh mengakses telefon anda secara fizikal.

PERIKSA - Pastikan anda berada di laman web rasmi WhatsApp Web. Berhati-hati dengan permintaan yang mencurigakan yang diterima melalui WhatsApp, walaupun mereka dihantar oleh kenalan WhatsApp anda.

Periksa peranti anda yang dipautkan dengan kerap. Untuk meniliti semua peranti yang dipautkan ke akaun anda, pergi ke tetapan WhatsApp > peranti yang dipautkan. Untuk mengeluarkan sebuah peranti yang dipautkan, klik pada peranti tersebut > log keluar.

BERITAHU – Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Jangan sekali-kali berkongsi kod pengesahan akaun WhatsApp anda, maklumat peribadi, butiran perbankan dan OTPs dengan sesiapa; laporkan sebarang transaksi menipu kepada bank anda dengan segera.

Untuk maklumat lanjut mengenai penipuan ini, sila layari SPF | News (police.gov.sg)

வெளியீடு எண். 34

10 நவம்பர் 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

போலி நண்பர் அழைப்பு மோசடி

வேலை மோசடி

முதலீட்டு மோசடி

இணைய வர்த்தக மோசடி (பல்வேறு வகைகள்)

தகவல் திருட்டு மோசடி

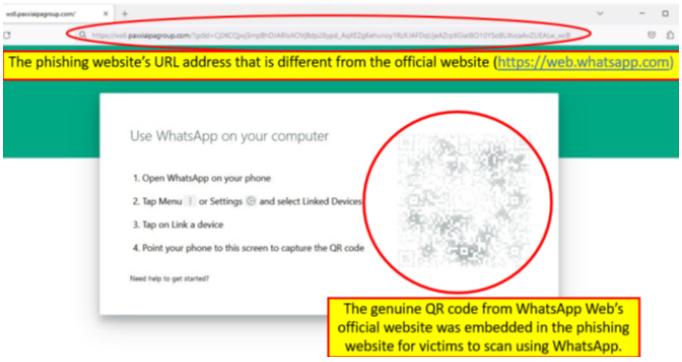
வாட்ஸ்ஆப் செயலியை இணையம் வழி (WhatsApp Web) பயன்படுத்துகிறீர்களா? உங்கள் வாட்ஸ்ஆப் கணக்கைப் பாதிக்கக்கூடிய புதிய தகவல் திருட்டு மோசடி வகை உள்ளது.

மோசடி உத்திகள்

வாட்ஸ்ஆப் செயலியை தங்கள் கணினி / டேப்லெட்டில் அணுக, பாதிக்கப்பட்டவர்கள் இணையத்தில் "வாட்ஸ்ஆப் வெப்" -ஐத் தேடுகின்றனர். இணையத்தள முகவரியைச் சரிபார்க்காமல் முதல் சில தேடல் முடிவுகளைக் கிளிக் செய்கின்றனர். மோசடிக்காரர்களால் அமைக்கப்பட்ட இந்த இணையத்தள முகவரிகள் "வாட்ஸ்ஆப் வெப்" - இன் ஒரே மாதிரியான தோற்றம் கொண்டிருப்பதுடன் அவற்றில் QR குறியீடும் இருக்கும்.

பாதிக்கப்பட்டவர் QR குறியீட்டை ஸ்கேன் செய்து, அவர்களின் கணினி / டேப்லெட்டில் வாட்ஸ்ஆப் அணுகலை அனுமதிப்பார்கள். ஆனால், அந்த தகவல் திருட்டுத் தளம் செயல்படாது. அதற்குப் பதிலாக, மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களுக்குத் தெரியாமலேயே அவர்களின் வாட்ஸ்ஆப் கணக்கின் அணுகலை பெறுவார்கள். கடன் / பண மாற்றல்களைக் கேட்பது அல்லது இணைய வங்கி / தனிப்பட்ட விவரங்களைக் கேட்பது போன்ற வழக்கத்திற்கு மாறான கோரிக்கைகளைக் கேட்க மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களின் தொடர்புகளை அணுகுவார்கள்.

தங்களுக்குக் கிடைத்த வழக்கத்திற்கு மாறான கோரிக்கைகள் குறித்து தங்களுடைய தொடர்புகள் தகவல் அளித்த பிறகே தங்களது வாட்ஸ்ஆப் கணக்கு பாதிக்கப்பட்டிருப்பதைப் பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.



[அதிகாரபூர்வ "வாட்ஸ்ஆப் வெப்" - ஐப் போல தோற்றமளிக்கும் தகவல் திருட்டு இணையத்தளத்தின் ஸ்கிரீன்ஷாட்]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்க - 'Two-Step Verification' அம்சத்தை செயல்படுத்துவதன் மூலம் உங்கள் வாட்ஸ்ஆப் கணக்கில் பாதுகாப்பு அம்சங்களைச் சேர்க்கவும். இதை வாட்ஸ்ஆப்-இன் செயலியின் அமைப்புகளில் செய்யலாம். ஒரு சாதனக் குறியீட்டை அமைத்து, உங்கள் தொலைபேசியை யார் நேரடியாக அணுக முடியும் என்பதை அறிந்து கொள்ளுங்கள்.

சரிபார்க்க - நீங்கள் வாட்ஸ்ஆப் வெப்" - இன் அதிகாரபூர்வ இணையத்தளத்தைப் பயன்படுத்துவதைச் சரிபார்க்கவும். உங்கள் வாட்ஸ்ஆப் தொடர்புகளால் அனுப்பப்பட்டாலும், வாட்ஸ்ஆப் மூலம் பெறப்படும் அசாதாரணமான கோரிக்கைகள் குறித்து எச்சரிக்கையாக இருங்கள்.

உங்கள் இணைக்கப்பட்ட சாதனங்களை தவறாமல் சரிபார்க்கவும். வாட்ஸ்ஆப் செயலியின் அமைப்புகள் > இணைக்கப்பட்ட சாதனங்கள் ஆகியவற்றுக்குச் சென்று உங்கள் கணக்குடன் இணைக்கப்பட்ட அனைத்து சாதனங்களையும் மறுஆய்வு செய்யுங்கள். இணைக்கப்பட்ட சாதனத்தை அகற்ற, சாதனத்தைக் கிளிக் செய்து, அதன் பிறகு வெளிச்செல்லவும்.

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். உங்கள் வாட்ஸ்ஆப் கணக்கின் சரிபார்ப்புக் குறியீடுகள், தனிப்பட்ட தகவல்கள், வங்கி விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் ஆகியவற்றை யாருடனும் பகிர்ந்து கொள்ளாதீர்கள். எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்குத் தெரிவிக்கவும்.

இந்த மோசடி குறித்த மேல் விவரங்களுக்கு, SPF | News (police.gov.sg) இணையத்தளத்தை நாடுங்கள்.