TRENDING SCAMS | IN THE PAST WEEK

Issue no. 15
30 June 2023

Scams to look out for

Job Scam

You receive a job offer promising high salary with little effort.

CHECK with official sources, such as the company's official website, to verify the job offer.

Fake Friend Call Scam

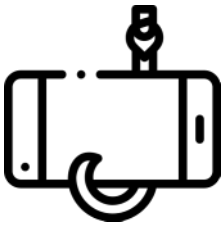
You receive a phone call from supposedly your "friend". You are asked to guess the caller's name and when you do so, the caller will assume this name. You are then asked to save the friend's new number. A few days later, this so-called friend will call you to ask for money to help him or her for an emergency, mother is in hospital etc.

CHECK with your friend through other means or call the original number to verify if indeed your friend had called you earlier.

Investment Scam

You are offered an investment with very high returns.

CHECK with official sources, such as the company's official website, to verify the deal. Do not be enticed by the initial positive gains. Do your own due diligence before you invest large sums of money.



Phishing Scam through Malware

You come across a deal for a product or service online. To facilitate payment, you are asked to click on a link and download an application from an unknown source.

ADD ScamShield app on mobile phone to detect scam messages and block scam calls. Do not click on links sent via any messaging and/or social media platforms by unknown sources. Only download and install applications from official application stores (i.e., Apple Store or Google Play Store).

E-Commerce Scam/ Others

You come across an attractive item or service (e.g., tour package, concert tickets or electronics) online and contact the seller through messaging app. After making payment, the item or service was not delivered. The seller becomes uncontactable.

CHECK the company's official website, seller's online reviews and ratings. Avoid making advance payments or direct bank transfer to anyone whom you do not know or have not met in person. Do not install any apps that sellers send you via links in messaging platforms. Only download apps from official application stores (Apple Store, Google Play Store).

⚠ Beware of malware enabled scams!

Scams Tactics

Scammers are tricking victims into downloading malicious applications to steal their money.

Victims are asked to download these applications (via URL links sent by scammers) when they order and make payment for goods or services found on social media platforms.

Once downloaded, scammers will be able to access victims' devices remotely to steal passcodes and banking information. Scammers would then access victims' bank accounts to make unauthorised transactions.

⚠ SCAM ALERT!

BEWARE of malicious apps

✗ DON'TS

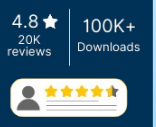
- **DO NOT** scan QR codes from **unknown sources**. Verify them with the authorities or business owners.

- **DO NOT** download **unknown apps** from a third-party website.

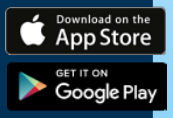
- **DO NOT** grant access to **persistent pop-ups**.

✓ DO'S

- **DO** check the app's **number of downloads and user reviews**.



- **DO** download apps only from **official app stores**.



- **DO be wary of requests** for banking credentials and money transfers.

ACT against scams now!

Visit **www.scamalert.sg** or call the Anti-Scam Hotline at **1800-722-6688**.
Get more cyber tips at:
https://www.go.gov.sg/bettercybersafe

Brought to you by:

CSA SINGAPORE

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

How to protect yourself

I Can ACT Against Scams

Remember to Add, Check and **Tell** (ACT) before making any decisions.

And never respond to urgent requests for information or money.

Always verify such requests with official websites or sources.

Get the latest advice. Visit www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688.

Report scams. Call the Police Hotline at 1800-255-0000 or submit information online at www.police.gov.sg/iwitness. All information will be kept strictly confidential.

Download the free ScamShield app

Detect, block and report scams with the ScamShield app.

GET IT ON Google Play | Download on the App Store

A crime prevention initiative by

NATIONAL CRIME PREVENTION COUNCIL

In collaboration with

SINGAPORE POLICE FORCE

SAFEGUARDING EVERY DAY

过去一周

15号刊

2023年6月30日

诈骗趋势

当心骗局

求职诈骗

您收到一份承诺只需付出很少努力就能获得高薪的工作机会。

查看官方消息，如公司的官方网站，以核实该工作机会。

假朋友来电

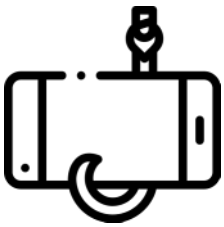
您接到来自"朋友"的电话。来电者在要求您猜他的姓名后会使用您所说的名字。来电者会要求您保存朋友的新电话号码。几天后，这所谓的朋友会拨电给您，以紧急事件或母亲住院等为由要求您提供经济援助。

通过其他沟通管道或原来的电话号码与您的朋友核实是否打电话给您。

投资诈骗

您收到了一项回报率非常高的投资机会。

查看官方消息，如公司的官方网站，以核实这笔交易。不要被初期的利润诱惑。在投入大笔资金前，请务必多加查证。



利用恶意软件的钓鱼诈骗

您在网上看到产品或服务的广告。为方便付款，您被要求点击一个链接并从一个未知来源下载一个应用程序。

在您的手机里下载 ScamShield 应用侦测诈骗短信和拦截诈骗电话。请勿点击由未知来源通过任何通讯和/或社交媒体平台发送的链接。只从官方应用程序商店（即Apple Store或Google Play Store）下载和安装应用程序。

电子商务/其他骗局

您在网上看到具吸引力的产品或服务（如：旅游配套、演唱会门票、电子产品）并通过通讯应用程序与卖家联系。付款后，您没有收到商品或服务。卖家也失联了。

查看公司的官方网站、卖家在线评论和评级。避免预付款项或通过银行直接转账给不认识或素未谋面的人。切勿安装任何由卖家通过通讯平台发送的链接下载的应用程序。只从官方应用程序商店（即Apple Store或Google Play Store）下载和安装应用程序。

⚠ 提防通过恶意软件的诈骗！

诈骗手法

骗子会诱骗受害者下载恶意应用程序以便盗取受害者的钱财。

在支付社交媒体平台上订购的商品或服务时，受害者被要求利用骗子所发送的链接下载这些应用程序。

下载后，骗子就能远程进入受害者的设备盗取密码和银行资料。骗子会登入受害者的银行户头进行未经授权的交易。

⚠如何保护自己

I Can ACT Against Scams

在做任何决定前，**请谨记下载、查看和告知(ACT)。**

千万别回复紧急的信息或金钱要求。

时刻与官方网站或可靠的管道核实此类请求。

上网 www.scamalert.sg 或拨打反诈骗热线 1800-722-6688，获取最新的防范骗案信息。

通报诈骗。拨打警方热线 1800-255-0000 或上网 www.police.gov.sg/iwitness 向警方提供诈骗线索。所有资料都将保密。

下载免费的防诈骗应用ScamShield
使用ScamShield应用以侦测，阻止及通报诈骗。

GET IT ON Google Play　Download on the App Store

防范罪案咨询由

NATIONAL CRIME PREVENTION COUNCIL

以及

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

协力带给您

TREND PENIPUAN | Isu no. 15

30 Jun 2023

SEPANJANG MINGGU LEPAS

Penipuan yang harus diawasi

Penipuan Pekerjaan

Anda menerima satu tawaran pekerjaan yang menjanjikan gaji yang lumayan dengan usaha yang sedikit.

PERIKSA dengan sumber-sumber rasmi, seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran pekerjaan tersebut.

Penipuan Panggilan Kawan Palsu

Anda menerima satu panggilan telefon daripada kononnya seorang "kawan". Anda diminta supaya meneka nama si pemanggil dan apabila anda berbuat demikian, pemanggil akan menggunakan nama yang anda teka tersebut. Anda kemudian diminta supaya menyimpan nombor baru si pemanggil tadi. Beberapa hari kemudian, pemanggil yang kononnya kawan anda ini akan menghubungi anda untuk meminta wang bagi menolongnya untuk suatu kecemasan, atau emaknya yang berada di hospital, dan sebagainya.

PERIKSA dengan kawan anda melalui cara lain atau telefon nombor asalnya untuk memastikan dia benar-benar telah menelefon anda tadi.

Penipuan Pelaburan

Anda ditawarkan satu pelaburan dengan pulangan yang sangat tinggi.

PERIKSA dengan sumber-sumber rasmi, seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran tersebut. Jangan tertarik dengan keuntungan awal yang positif. Lakukan pemeriksaan yang teliti dan wajar sebelum anda melaburkan wang dengan jumlah yang besar.

Penipuan Pancingan Data Melalui Perisian Hasad

Anda ternampak satu tawaran untuk sebuah produk atau khidmat dalam talian. Untuk memudahkan pembayaran, anda diminta supaya mengklik satu pautan dan memuat turun satu aplikasi dari sumber yang tidak diketahui.

MASUKKAN aplikasi ScamShield ke telefon bimbit anda untuk menyekat panggilan penipuan dan menapis SMS penipuan. Jangan klik pada pautan yang dihantar melalui mana-mana platform pesanan dan/atau media sosial oleh sumber yang tidak diketahui. Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi (misalnya, Gedung Apple atau Gedung Google Play).

Penipuan E-Dagang/ Lain-lain

Anda ternampak satu barang atau khidmat yang menarik (misalnya, pakej pelancongan, tiket konsert atau elektronik) dalam talian dan menghubungi penjual melalui aplikasi pesanan. Setelah membuat pembayaran, barang atau khidmat tersebut tidak dihantar. Penjual tidak dapat dihubungi.

PERIKSA laman web rasmi syarikat tersebut, ulasan dan penilaian dalam talian penjual. Elakkan dari membuat bayaran pendahuluan atau pemindahan bank secara langsung kepada sesiapapun yang tidak anda kenali atau bertemu secara peribadi. Jangan memasang sebarang aplikasi yang dihantar oleh penjual melalui pautan di platform pesanan. Muat turun aplikasi hanya daripada gedung aplikasi rasmi (Gedung Apple, Gedung Google Play).

Berhati-hati terhadap penipuan yang disebabkan oleh perisian hasad!

Taktik Penipuan

Penipu menipu mangsa untuk memuat turun aplikasi berniat jahat untuk mencuri wang mereka.

Mangsa diminta memuat turun aplikasi ini (melalui pautan URL yang dihantar oleh penipu) apabila mereka memesan dan membuat pembayaran untuk barangan atau perkhidmatan yang terdapat di platform media sosial.

Setelah dimuat turun, penipu akan dapat mengakses peranti mangsa dari jauh untuk mencuri kod laluan dan maklumat perbankan. Penipu kemudiannya akan mengakses akaun bank mangsa untuk membuat transaksi tanpa kebenaran.

AMARAN PENIPUAN!

BERHATI-HATI dengan aplikasi berniat jahat

Apa yang tidak boleh dilakukan

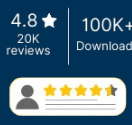
- **JANGAN** mengimbas kod QR dari **sumber yang tidak diketahui.** Sahkan mereka dengan pihak berkuasa atau pemilik perniagaan.

- **JANGAN** muat turun aplikasi yang tidak diketahui daripada laman web pihak ketiga.

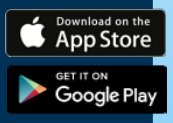
- **JANGAN** berikan akses kepada **pop-up berterusan.**

Apa yang harus dilakukan

- **HARUS** periksa **bilangan muat turun** aplikasi itu **dan ulasan penggunanya.**



- **HARUS** muat turun aplikasi hanya daripada **gedung aplikasi rasmi.**



- **HARUS berhati-hati dengan permintaan** untuk butiran perbankan dan pemindahan wang.

Bertindak (ACT) terhadap Penipuan sekarang!

Lawati **www.scamalert.sg** atau hubungi Talian Bantuan Anti-Penipuan di **1800-722-6688**.

Dapatkan lebih banyak panduan siber di:
https://www.go.gov.sg/bettercybersafe

Dibawakan kepada anda oleh:

CSA SINGAPORE

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

⚠ Bagaimana melindungi diri anda

I Can ACT Against Scams

Ingatlah untuk Masukkan (Add), Periksa (Check) dan **Beritahu (Tell)** atau ACT sebelum membuat sebarang keputusan.

Dan jangan membalas sebarang permintaan mendesak untuk maklumat atau wang.

Pastikan selalu kesahihan permintaan-permintaan tersebut daripada laman-laman web atau sumber-sumber rasmi.

Dapatkan nasihat terkini. Lawati www.scamalert.sg atau hubungi Talian Bantuan Anti-Penipuan di 1800-722-6688.

Adukan penipuan. Panggil Talian Hotline Polis di 1800-255-0000 atau hantarkan maklumat dalam talian di www.police.gov.sg/iwitness. Semua maklumat akan dirahsiakan sama sekali.

Muat turun aplikasi percuma yang dipanggil ScamShield
Kesan, sekat dan adu penipuan dengan aplikasi ScamShield.

GET IT ON Google Play Download on the App Store

Sebuah inisiatif pencegahan jenayah oleh

NATIONAL CRIME PREVENTION COUNCIL

Dengan kerjasama

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

கடந்த வாரத்தின் | முன்னணி மோசடிகள்

வெளியீடு
எண். 15
30 ஜூன் 2023

எச்சரிக்கையாக இருக்க வேண்டிய மோசடிகள்

வேலை மோசடி

நீங்கள் சிறிதும் முயற்சி செய்யாமல், அதிக சம்பளம் வழங்குவதாக உறுதியளிக்கும் ஒரு வேலை வாய்ப்பைப் பெறுகிறீர்கள்.

வேலை வாய்ப்பை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் **சரிபார்க்கவும்**.

போலி நண்பர் அழைப்பு மோசடி

உங்களுக்கு ஒரு "நண்பரிடமிருந்து" தொலைபேசி அழைப்பு வருகிறது. அழைப்பவரின் பெயரை யூகிக்க நீங்கள் கேட்கப்படுகிறீர்கள். அவ்வாறு நீங்கள் செய்யும்போது, அழைப்பவர் நீங்கள் குறிப்பிட்ட பெயரை ஏற்றுக்கொள்வார். பின்னர் அவர்களின் புதிய எண்ணைத் தொலைபேசியில் பதிவு செய்துக்கொள்ளும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள். சில நாட்களுக்குப் பிறகு, உங்கள் நண்பர் என்று தன்னை அறிமுகப்படுத்திக் கொண்ட இந்த நபர், அவசர நிலைமைக்கு அவருக்கு உதவ பணம் கேட்டு உங்களை அழைப்பார். ஒரு உதாரணத்திற்கு, அவரது தாயார் மருத்துவமனையில் இருக்கிறார் என்று கூறலாம்.

உங்கள் நண்பர் உங்களை சற்றுமுன் அழைத்திருந்தார்களா என்பதை மற்ற வழிகள் மூலமாகவோ அல்லது அவர்களின் அசல் எண்ணிலோ தொடர்புக்கொண்டு **சரிபார்க்கவும்**.

முதலீட்டு மோசடி

மிக உயர்ந்த வருவாய்யைக் கொண்ட ஒரு முதலீடு உங்களுக்கு வழங்கப்படுகிறது.

ஒப்பந்தத்தை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் **சரிபார்க்கவும்**. ஆரம்ப ஆதாயங்களைக் கண்டு கவர்ந்துவிடாதீர்கள். நீங்கள் ஒரு பெரியத் தொகையை முதலீடு செய்வதற்கு முன்பு உங்கள் சொந்த சோதனைகளை மேற்கொள்ளுங்கள்.

தீங்கிழைக்கும் மென்பொருள் மூலம் தகவல் திருட்டு மோசடி

இணையத்தில் ஒரு நல்ல பொருளையோ சேவையையோ காண்கிறீர்கள். கட்டணம் செலுத்துவதை எளிதாக்க, நீங்கள் ஓர் இணைப்பை கிளிக் செய்து அறியப்படாத தளத்திலிருந்து ஒரு செயலியைப் பதிவிறக்கம் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள்.

மோசடி அழைப்புகள் மற்றும் மோசடி குறுஞ்செய்திகளைத் தடுக்க கைபேசியில் ஸ்கேம்ஷீல்ட் செயலியைச் **சேர்க்கவும்**. செய்தி அனுப்பும் தளங்கள் அல்லது சமூக ஊடகத் தளங்கள் வழியாக தெரியாதவர்களால் அனுப்பப்படும் எந்தவொரு இணைப்புகளையும் கிளிக் செய்ய வேண்டாம். அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து (அதாவது, ஆப்பிள் ஸ்டோர் அல்லது கூகிள் பிளே ஸ்டோர்) மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யவும்.

இணைய வர்த்தக மோசடி / மற்றவை

நீங்கள் இணையம்வழி ஒரு கவர்ச்சிகரமான பொருள் அல்லது சேவையைப் (எ. கா. சுற்றுப்பயணத் தொகுப்பு, இசை நிகழ்ச்சி நுழைவுச்சீட்டுகள் அல்லது மின்னணுவியல் பொருட்கள்) பார்த்து, செய்தி அனுப்பும் செயலி மூலம் விற்பனையாளரைத் தொடர்புகொள்கிறீர்கள். பணம் செலுத்திய பிறகு, பொருள் அல்லது சேவை வழங்கப்படவில்லை. விற்பனையாளரையும் தொடர்பு கொள்ள முடியவில்லை.

நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம், விற்பனையாளரின் இணைய மதிப்பாய்வுகள் மற்றும் தரநிலைகளை **சரிபார்க்கவும்**. உங்களுக்குத் தெரியாத அல்லது நேரில் சந்திக்காத எவருக்கும் முன்கூட்டியே பணம் செலுத்துவதையோ அல்லது நேரடி வங்கி பரிமாற்றம் செய்வதையோ தவிர்க்கவும். செய்தி அனுப்பும் தளங்களில் உள்ள இணைப்புகள் வழியாக விற்பனையாளர்கள் உங்களுக்கு அனுப்பும் எந்தவொரு செயலிகளையும் நிறுவாதீர்கள். அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து (ஆப்பிள் ஸ்டோர் அல்லது கூகிள் பிளே ஸ்டோர்) மட்டுமே செயலிகளை பதிவிறக்கம் செய்யுங்கள்.

தீங்கு விளைவிக்கும் மென்பொருள் மூலம் நடத்தப்படும் மோசடிகள் குறித்து எச்சரிக்கையாக இருங்கள்!

மோசடி உத்திகள்

மோசடிக்காரர்கள் பணத்தைத் திருடுவதற்கு, தீங்கிழைக்கும் செயலிகளைப் பதிவிறக்கம் செய்யும்படி பாதிக்கப்பட்டவர்களை ஏமாற்றுகின்றனர்.

பாதிக்கப்பட்டவர்கள் சமூக ஊடகத் தளங்களில் காணப்படும் பொருட்கள் அல்லது சேவைகளுக்கு ஆர்டர் செய்து பணம் செலுத்தும்போது இந்த செயலிகளை (மோசடிக்காரர்களால் அனுப்பப்பட்ட வலைத்தள முகவரிகளின் இணைப்புகள் வழியாக) பதிவிறக்கம் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறார்கள்.

பதிவிறக்கம் செய்யப்பட்டவுடன், மோசடிக்காரர்கள் கடவு எண்கள் மற்றும் வங்கித் தகவல்களைத் திருட பாதிக்கப்பட்டவர்களின் சாதனங்களை தொலைவிலிருந்து அணுக முடியும். மோசடிக்காரர்கள், பாதிக்கப்பட்டவர்களின் வங்கிக் கணக்குகளை அணுகி, அனுமதிக்கப்படாத பரிவர்த்தனைகளைச் செய்வார்கள்.

மோசடி எச்சரிக்கை!

தீங்கிழைக்கும் செயலிகள் குறித்து எச்சரிக்கையாக இருங்கள்

செய்யக்கூடாதவை

- **அறியப்படாத மூலங்களிலிருந்து** அனுப்பப்படும் விரைவுத் தகவல் குறியீடுகளை ஸ்கேன் **செய்ய வேண்டாம்**. அதிகாரிகள் அல்லது வணிக உரிமையாளர்களுடன் அவற்றை சரிபார்க்கவும்.

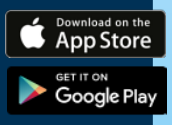
- **அறியப்படாத செயலிகளை** மூன்றாம் தரப்பு இணையத்தளத்திலிருந்து பதிவிறக்கம் **செய்ய வேண்டாம்.**

- **தொடர்ச்சியான பாப் அப்களுக்கு** அணுகலை வழங்க **வேண்டாம்.**

செய்ய வேண்டியவை

- செயலியின் **பதிவிறக்கங்கள் மற்றும் பயனர் மதிப்பாய்வுகளின் எண்ணிக்கையை சரிபார்க்கவும்.**

- **அதிகாரபூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து** மட்டுமே செயலிகளைப் பதிவிறக்கம் **செய்யுங்கள்.**



- வங்கி சான்றுகள் மற்றும் பணப் பரிமாற்றங்களுக்கான **கோரிக்கைகள் குறித்து எச்சரிக்கையாக இருங்கள்.**

மோசடிகளுக்கு எதிராக இப்போதே செயல்படுங்கள் (ACT)!

www.scamalert.sg இணையத்தளத்தை நாடுங்கள் அல்லது 1800-722-6688 என்ற மோசடி தடுப்பு உதவி எண்ணை அழையுங்கள்.

கூடுதல் இணையக் குறிப்புகளைப் பெறுவதற்கு:
https://www.go.gov.sg/bettercybersafe

உங்களுக்கு வழங்குவது:

CSA SINGAPORE

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

எப்படி உங்களைப் பாதுகாத்துக்கொள்வது

எந்தவொரு முடிவையும் எடுப்பதற்கு முன்பு **சேர்க்க, சரிபார்க்க** மற்றும் **சொல்ல** (ACT) **நினைவில் கொள்ளுங்கள்.**

தகவல் அல்லது பணத்திற்கான அவசர கோரிக்கைகளுக்கு ஒருபோதும் பதிலளிக்காதீர்கள்.

அத்தகைய கோரிக்கைகளை அதிகாரபூர்வ இணையத்தளம் அல்லது ஆதாரங்களுடன் எப்போதும் சரிபார்த்துக்கொள்ளுங்கள்.

ஆக அண்மைய ஆலோசனையைப் பெறுங்கள். www.scamalert.sg இணையத்தளத்தை நாடுங்கள் அல்லது 1800-722-6688 என்ற மோசடி தடுப்பு உதவி எண்ணை அழையுங்கள்.

மோசடிகளை புகார் செய்யுங்கள். 1800-255-0000 என்ற காவல்துறை நேரடித் தொலைபேசி எண்ணை அழையுங்கள் அல்லது www.police.gov.sg/iwitness என்ற இணையதளத்தில் தகவல்களை சமர்ப்பிக்கலாம். அனைத்து தகவல்களும் ரகசியமாக வைத்திருக்கப்படும்.

ஸ்கேம்ஷீல்ட் செயலியை இலவசமாக பதிவிறக்கம் செய்யுங்கள்.
ஸ்கேம்ஷீல்ட் செயலியைப் பயன்படுத்தி மோசடிகளைக் கண்டறிந்து, தடுத்து, அவற்றைப் பற்றி புகார் செய்யுங்கள்.

GET IT ON Google Play | Download on the App Store

ஒரு குற்றத் தடுப்பு முன்முயற்சி

NATIONAL CRIME PREVENTION COUNCIL

இணைந்து வழங்குபவர்கள்

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY