SECURITY MATTERS
NEWSLETTER

STAY AWAY FROM THE BAIT. DON'T LET ANYONE PHISH YOU!

VOL 11 • APRIL 2023

Everyone is susceptible to a phishing attack. Phishing is a form of cybercrime in which the scammer asks you to provide them with your personal information through email, telephone, or text message by pretending to be someone else. Phishing scams are becoming more sophisticated. Hackers can purchase phishing kits, which clone popular websites and operate from temporary servers, from underground dealers for relatively small prices without end user awareness, any technical control can be defeated. There are several forms of phishing attacks. Nevertheless, all these different types of phishing attacks have a common objective - tries to get the victim to hand over sensitive information or download malware.

Common types of phishing attacks:

- Email phishing
- Spear phishing
- Smishing
- Vishing

Common phishing ploys:

- Government impostor scams
- Fake person scams
- Love/romance scams
- Employment scams
- Prize/giveaway scams
- Debt collection/settlement scams
- Purchase/delivery scams
- Fake refund/over payment scams
- Fake fraud alert from bank
- "Family emergency" text
- Text with bills/invoices you don't recognize

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me
Help desk (Signal & WhatsApp): +6011 6516 6310

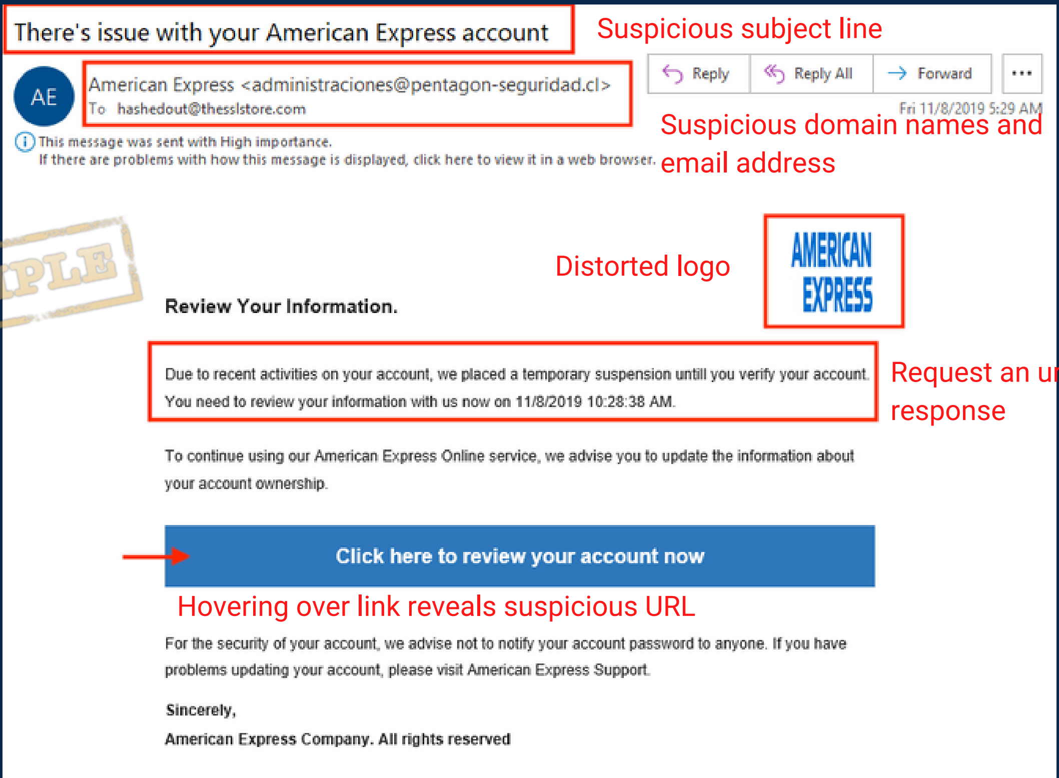
More information about Security Matters, visit www.securitymatters.asia
✉ info@securitymatters.asia
@secm8
@sec_matters

SECURITY MATTERS
NEWSLETTER

STAY AWAY FROM THE BAIT. DON'T LET ANYONE PHISH YOU!

VOL 11 • APRIL 2023

How to identify an email phishing attempt?



There's issue with your American Express account

Suspicious subject line

AE American Express <administraciones@pentagon-seguridad.cl>
To hashedout@thesslstore.com

Fri 11/8/2019 5:29 AM

Suspicious domain names and email address

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Distorted logo

Review Your Information.

Due to recent activities on your account, we placed a temporary suspension untill you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

Request an urgent response

To continue using our American Express Online service, we advise you to update the information about your account ownership.

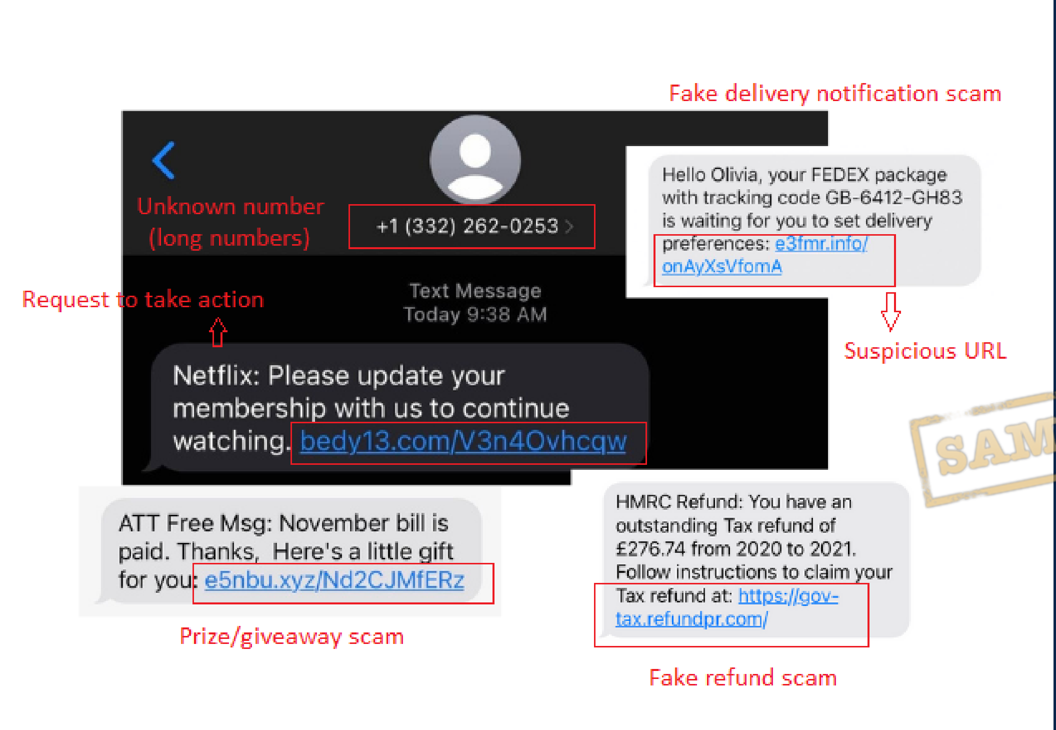
Click here to review your account now

Hovering over link reveals suspicious URL

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,
American Express Company. All rights reserved

How to identify a SMS phishing attempt?



Fake delivery notification scam

Unknown number (long numbers)

+1 (332) 262-0253 >

Text Message
Today 9:38 AM

Request to take action

Netflix: Please update your membership with us to continue watching. bedy13.com/V3n4Ovhcqw

Hello Olivia, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: e3fmr.info/onAyXsVfomA

Suspicious URL

ATT Free Msg: November bill is paid. Thanks, Here's a little gift for you: e5nbu.xyz/Nd2CJMfERz

Prize/giveaway scam

HMRC Refund: You have an outstanding Tax refund of £276.74 from 2020 to 2021. Follow instructions to claim your Tax refund at: https://gov-tax.refundpr.com/

Fake refund scam

SECURITY MATTERS

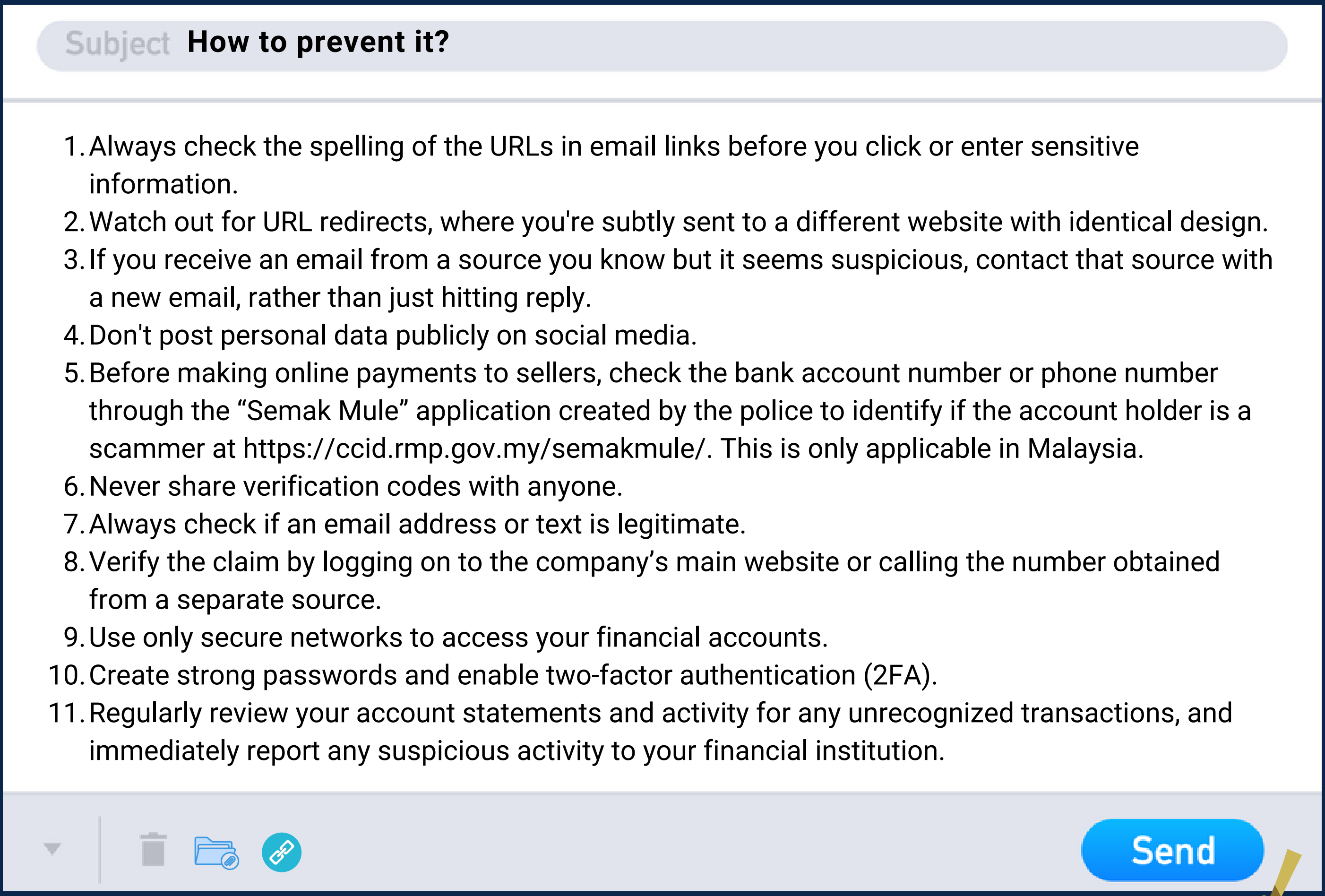
General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me
Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8
@sec_matters

SECURITY MATTERS
NEWSLETTER

STAY AWAY FROM THE BAIT. DON'T LET ANYONE PHISH YOU!

VOL 11 • APRIL 2023



Subject **How to prevent it?**

1. Always check the spelling of the URLs in email links before you click or enter sensitive information.
2. Watch out for URL redirects, where you're subtly sent to a different website with identical design.
3. If you receive an email from a source you know but it seems suspicious, contact that source with a new email, rather than just hitting reply.
4. Don't post personal data publicly on social media.
5. Before making online payments to sellers, check the bank account number or phone number through the "Semak Mule" application created by the police to identify if the account holder is a scammer at https://ccid.rmp.gov.my/semakmule/. This is only applicable in Malaysia.
6. Never share verification codes with anyone.
7. Always check if an email address or text is legitimate.
8. Verify the claim by logging on to the company's main website or calling the number obtained from a separate source.
9. Use only secure networks to access your financial accounts.
10. Create strong passwords and enable two-factor authentication (2FA).
11. Regularly review your account statements and activity for any unrecognized transactions, and immediately report any suspicious activity to your financial institution.

What should I do if I clicked on a scam link?

1. Disconnect from your Wi-Fi or mobile network immediately.
2. Back up your sensitive files.
3. Scan your device for malware or viruses immediately.
4. Change your passwords immediately.
5. Setting up 2FA and using a password manager on all your accounts.
6. If you're a victim of a bank fraud alert , call your bank immediately to report the situation.
7. Report the scams to the relevant channels/platforms.
8. Take action and block the number sending you spam.

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me
Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8
@sec_matters

Related News

Chinese shopping app Pinduoduo with over 7 million users cab spy on people

Pinduoduo, one of China's most popular shopping apps, has been accused of spying on users by cybersecurity researchers. The online shopping app was recently suspended by Google due to alleged malware found in certain versions of it.
Read more: http://bit.ly/43k0zto

Beware of new YouTube phishing scam using authentic email address

Watch out for a new YouTube phishing scam and ignore any email from YouTube that claims to provide details about “Changes in YouTube rules and policies | Check the Description.”
Read more: https://bit.ly/41f7hj5

Scammers on the line: How to protect yourself against scam calls

From prizes to threats, scammers keep finding new ways to get into our pockets. A convincing narrative or an intricate scheme can convince many to part with their money. Many don’t realise they’ve been scammed until it’s too late.
Read more:http://bit.ly/3KoZpEd

Most cell phone numbers in Malaysia are leaked and sold to scammers

73% of cell phone numbers in Malaysia are leaked or sold to scammers, equivalent to more than 21 million people connected to local telcos. Other top private information leaks are login passwords and names for Malaysia, Taiwan, and Thailand, followed by the address, country, date of birth, and email leaks.
Read more: http://bit.ly/3mjXmcO

Beware of 'juice jacking' when charging devices with public USB ports

The FBI is alerting people to the risks involved in using USB charging ports available in public spaces. Some of these can be corrupted, and pose a danger if you happen to plug your smartphone or tablet into them. This phenomenon, called ‘juice jacking’, can lead to the theft of personal data.
Read more: http://bit.ly/3UttrLD

WhatsApp introduces new device verification feature to prevent account takeover attacks

WhatsApp is debuting three new security features that it says will help protect users' accounts from being used for impersonations. Additional verification on the world's most popular messaging app will ensure both parties in each conversation will know they are talking to the right person.
Read more: https://bit.ly/3A1RSGI

AI can crack most passwords in less than a minute

Think your password is strong? Now might be a good time to update your password to something longer and more complex, as experts have found AI systems are able to crack almost all passwords easily. Seven-character passwords were cracked in under six minutes, even if they had numbers, upper and lowercase letters, and symbols.
Read more: https://bit.ly/3KMv42G

YouTube is being attacked by hackers using vicious malware

Using the content generated by AI on YouTube, users are being scammed into downloading malware that is capable of stealing their information which may be sensitive. The malware gets access to the user's information like account numbers, passwords, credit card info etc, and is then misused by the hacker's Control server and Command.
Read more: http://bit.ly/3JgNaJm

Alert: Scammers pose as ChatGPT in new phishing scam

This phishing scam exploits the popularity of the AI-based ChatGPT chatbot to steal funds and harvest the personal and financial details of users. In this scam, the primary targets were found in Ireland, Australia, Germany, Denmark and Netherlands.
Read more: https://bit.ly/44baQsu

Google Authenticator major update rings Cloud backup feature

Google Authenticator provides additional security for various applications by providing authentication codes for every sign-in. If a user loses the device in which this Google authenticator is installed, they face an account lockout as they cannot log in without the authentication codes. However, Google has now released a new feature in Google authenticator that will help overcome the problem of devices lost/stolen.
Read more: https://bit.ly/3n9pL5x

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me
Help desk (Signal & WhatsApp): +6011 6516 6310

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters