Republic of the Philippines
Supreme Court
Manila

ADMINISTRATIVE ORDER NO. 150-2023

RE: PROPER CYBER HYGIENE IN THE JUDICIARY

In view of the recent ransomware attacks targeting various government institutions, it is imperative for the Judiciary to bolster our cybersecurity measures and practice proper cyber hygiene. This administrative order is issued to establish guidelines to enhance our cybersecurity practices, protect sensitive data, and minimize the risk of cyber threats. Thus, ALL courts, judiciary offices, justices, judges, court officials, and employees are hereby **DIRECTED** to adhere to strict security protocols, remain vigilant in identifying and reporting any suspicious activities, and adopt the below guidelines:

1. EMAIL SAFETY

One of the most common ways of ransomware attacks is done through phishing emails which usually contain malicious links or attachments. Do not open these links or attachments unless they have been verified to be legitimate.

Below are some recommendations to help prevent Judiciary personnel from becoming victims of phishing:

a. **Check the Sender's Email Address**: Examine the sender's email address carefully. Phishers often use email addresses that look similar to ones used by legitimate organizations but may have small misspellings or inconsistencies. Always take a close look at the sender's display name when checking the legitimacy of an email. Most companies use a single domain for their URLs and emails, so a message that originates from a different domain is a red flag.

b. **Protect Your Personal Information:** Legitimate organizations typically do not request sensitive information like passwords, or credit card details via email. If in doubt, verify with the company itself to avoid any potential issues.

c. **Verify Links Before Clicking**: As a general rule, DO NOT click on links or download files even if they come from seemingly "trustworthy" sources. Hover your mouse over links in the email without clicking. Check if the URL matches the legitimate website's address. If it doesn't, it's likely a phishing attempt.

d. **Look for Misspellings and Grammar Errors**: Phishing emails often contain typos, grammatical errors, or awkward language. Legitimate companies typically have professional communication.

e. **Be Cautious with Urgent Messages:** Phishers often create a sense of urgency or fear to make you act quickly without thinking. Take your time to evaluate the email.

f. **Check for Generic Greetings:** Phishing emails are designed to be sent to a large number of people and often use generic greetings like "Dear User".

g. **Double-Check Attachments**: Do not open email attachments from unknown or unexpected sources. They may contain malware. If your email provider supports it, have all attachments scanned for viruses before you open them.

h. **Report Suspicious Emails:** If you receive a suspicious email, report it immediately. If it seems suspicious, it probably is. If you suspect that the sender's email address has been compromised, contact them through alternate modes of communication to check the authenticity of what you received.

Copies of related cybersecurity advisories and issuances on phishing that were previously issued by the Management Information Systems Office (MISO) are attached herewith as ***Annex A* series.**

2. PASSWORD SECURITY

Password security is of paramount importance in safeguarding your online accounts and personal information. A strong password is one that is easy for you to remember but difficult for others to guess. Below are some of the most important things to remember when creating a password:

a. Never Use Personal Information: Do not use your name, birthday, username, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.

b. Use a Longer Password: Longer passwords are more secure. Your password should be at least twelve (12) characters long, which contains numbers, symbols, and both uppercase and lowercase letters, if allowed by the service.

These tips can help you create strong passwords that are easier to remember. Try to use:

- A lyric from a song or poem
- A meaningful quote from a movie or speech
- A passage from a book
- A series of words that are meaningful to you
- An abbreviation: Make a password from the first letter of each word in a sentence

Avoid choosing passwords that could be guessed by:

- People who know you
- People looking at easily accessible info (like your social media profile)

c. **Do Not Use the Same Password for Each Account**: Never reuse passwords across multiple accounts. Each account should have its own unique password.

d. **Avoid Dictionary Words**: Refrain from using dictionary words as your passwords as they are susceptible to dictionary attack. For example, *justice123* would be a weak password.

e. **Consider Passphrases**: Instead of a single word, consider using passphrases:a sequence of random words or a meaningful phrase. Passphrases can be both strong and easy to remember.

f. **Use a Password Manager:** If you have trouble remembering multiple passwords, consider using a trusted password manager. These tools make managing numerous unique passwords more convenient.

g. **Do not Share Your Passwords with Anyone:** Never give your password to people who call you on the phone or send unsolicited email, even if they claim to be from the MISO, from your bank, or other trusted institutions.

h. **Secure Your Written Passwords**: If you need to write any of your passwords down, don't leave it on your computer or desk. Make sure any written passwords are stored somewhere that is secured.

i. **Enable Multi-factor Authentication (MFA).** Attached as ***Annex B*** series is a step by step guide on how to enable MFA on your accounts.

3. SOFTWARE AND SYSTEM UPDATES

System updates are essential for the smooth and secure operation of your devices whether it is a laptop, desktop, smartphone, tablet, or any other electronic device. Court personnel shall ensure that their operating system, applications, and security software remain up to date. Regularly check for updates to ensure that the latest security patches remain installed. Attached as ***Annex C*** is Cybersecurity Advisory No. 2023-02 that was issued by the MISO last 13 September 2022 for reference.

Here is the step-by-step guide on how to check for system updates:

- For Windows
    - Select **Start**
    - On the search bar, type **Windows Update**
    - Select **Windows Update**
    - **Windows Update** window will show
    - Click **Check for Updates**
    - *If there is an update available, it will start installing. If there are no updates, it will say that your PC is up to date.*

- For Apple/Mac
    - Choose Apple menu, click **System Settings**
    - Click **General** in the sidebar
    - Click **Software Update**

Likewise, below is the step-by-step guide on how to check if Microsoft Defender anti-virus is enabled on a Windows computer:

- Go to **Start** and select **Settings**
- Select **Update and Security**
- Choose **Windows Security**
- Look for **Virus and Threat Protection > Microsoft Defender** enabled

Alternatively, below is a list of free third-party anti-virus applications that may be downloaded and installed in lieu of Microsoft Defender on your PC or XProtect on Mac:

- Avast Security - https://www.avast.com/en-ph/
- AVG Antivirus - https://www.avg.com/en-ww/
- Bitdefender Antivirus - https://www.bitdefender.com/solutions/antivirus.html
- Malwarebytes - https://www.malwarebytes.com/
- Sophos Home - https://home.sophos.com/en-us
- TrendMicro - https://www.trendmicro.com/en_za/forHome/products/free-tools.html

4. DATA BACKUP

Data back-up is a critical practice to protect your important file and ensure you can recover them in case of data loss. Court personnel may follow the 3-2-1 backup rule to ensure data redundancy, resilience, and availability in case of hardware failure, data corruption, or catastrophic events:

a. **3 Copies of Your Data**: Maintain three separate copies of your data. This means you have the original data on your primary device (e.g., laptop, tablet, mobile phone), and two additional copies in different locations or on different media.

b. **2 Backup Media/Formats**: Backups should be stored on at least two different types of media or formats (*Ex. one copy on an external hard drive and another in the cloud*). This avoids media failure or compatibility issues.

c. **1 Offsite Backup**: At least one of the three copies of data should be stored offsite, in a different physical location from your primary data and your backup.

5. SAFE INTERNET USAGE

Safe internet usage is essential to protect your personal information, privacy, and security. Avoid visiting high-risk websites and downloading files from untrusted sources, such as torrent sites or unverified software repositories. Only download software or files from reputable sources. Only utilize the judiciary-approved and secure file-sharing platforms for work-related activities.

6. DEVICE SECURITY

Device security is crucial for protecting your online accounts. Court personnel are instructed to lock their computer and devices when not in use, especially in public or shared spaces. If logging into an account on a shared computer or device, log out immediately once the activity is completed. Immediately report lost or stolen devices to the MISO to prevent data leaks or breaches.

7. IMMEDIATELY REPORT SUSPICIOUS ACTIVITIES

Reporting suspicious activities within your online accounts can help maintain a safe online environment. Immediately report any suspicious emails, links, ads, or attachments to the MISO. Prompt reporting is key to the prevention of potential threats.

PHILHEALTH DATA LEAK

In view of the recent data breach involving Philippine Health Insurance Corporation (PHILHEALTH), Judiciary employees may access the site created by the National Privacy Commission (https://philhealthleak.privacy.gov.ph) to check if their data are among those affected by the said data breach.

ARTIFICIAL INTELLIGENCE (AI) IMAGE GENERATORS

The use of AI in digital applications is becoming increasingly popular. The online trending digital application that uses AI which requires its users to submit several photos of themselves to generate an enhanced portrait, however, poses significant privacy and security risks. This application compiles its users' data and creates a digital person that mimics how a real individual speaks and moves. While this may seem harmless and amusing, it can be maliciously used to create fake profiles that can lead to identity theft, social engineering, phishing attacks, and other malicious activities. There has already been a report of such a case.

It is important for users to be aware of the potential risks associated with such applications. Judiciary employees should be cautious when sharing their personal information online and they should only use applications from trusted sources. Additionally, Judiciary employees should read the privacy policy of any application before using it and should be aware of how their data will be used. By taking these precautions, Judiciary employees can help protect themselves from potential privacy and security risks.

If you require any assistance regarding this matter, you may contact the Management Information Systems Office (MISO) at 02-8525-7157, 02-8525-7164, or email at support.email@judiciary.gov.ph.

For information and guidance.

20 October 2023

MARVIC M.V.F. LEONEN
Acting Chief Justice
(Per Special Order No. 3033
dated 13 October 2023)

ANNEX A-1

CYBERSECURITY ADVISORY NO. 2023-02

Please be wary of the below phishing email purporting to be from the Landbank of the Philippines:

Important reminders:

- Always check/verify the sender's email address: malicious actions use fake email addresses and try to make it appear as if the email is from a legitimate source. Always check the sender's email address and verify it before clicking on any links or providing any information.
- Phishing emails often contain spelling and grammatical errors. Legitimate emails from reputable sources typically have a professional tone and are free of spelling and grammatical errors.
- DO NOT provide sensitive information: Never provide your personal or financial information in response to an unsolicited email or phone call. Legitimate companies will **never** ask for this information via email or phone.
- Use multi-factor authentication: multi-factor authentication adds an extra layer of security to your accounts by requiring a second form of verification in addition to your password. This makes it harder for cybercriminals to access your accounts.
- Keep your software up to date: Keeping your software up to date helps to patch security vulnerabilities that cybercriminals can exploit to carry out phishing attacks.

Should you encounter phishing emails, please immediately report them as phishing or spam.

To report a phishing email, you can follow these steps:

1. Open the subject email you want to report.
2. Click on the dropdown menu in the toolbar at the top of the email.
3. Select “Report Phishing” or “Report as Spam” from the dropdown menu.
4. Click “Report” to send the report.

You may likewise contact the Management Information Systems Office at miso.sc@judiciary.gov.ph for assistance.

For your information and guidance.

Thank you.

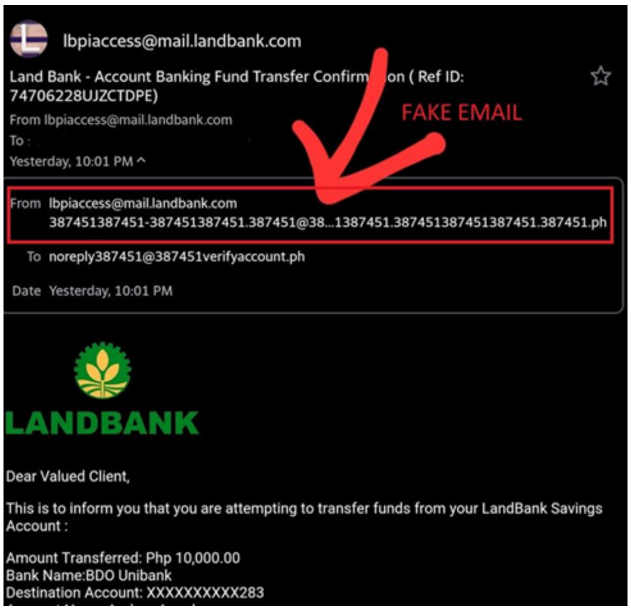
ANNEX A-2

CYBERSECURITY ADVISORY NO. 2022-07

Phishing emails purporting to be from Landbank of the Philippines

Please be informed of phishing emails purporting to be notifications from Landbank of the Philippines of fund transfer attempts. The said phishing emails contain a button for the victims to "cancel" a supposed online fund transfer transaction. Please see attached for Recommendations on how to avoid this kind of Email Phishing.

Below are the screenshots of the said phishing emails for reference:



lbpiaccess@mail.landbank.com

Land Bank - Account Banking Fund Transfer Confirm on (Ref ID: 74706228UJZCTDPE)

From lbpiaccess@mail.landbank.com

To :

Yesterday, 10:01 PM ^

From lbpiaccess@mail.landbank.com
387451387451-387451387451.387451@38...1387451.387451387451387451.387451.ph

To noreply387451@387451verifyaccount.ph

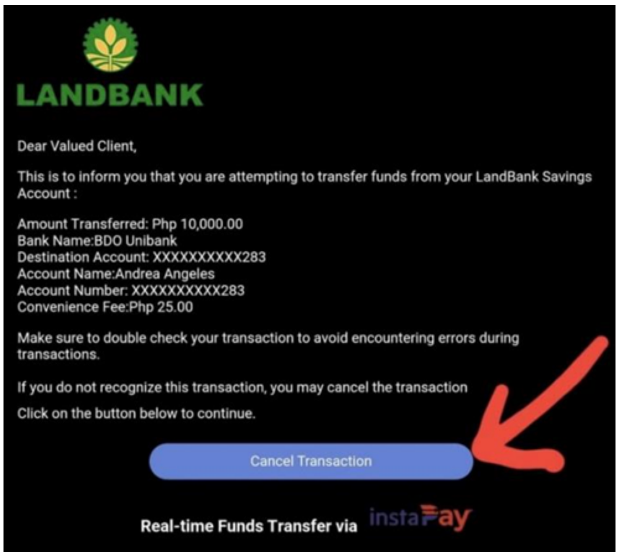
Date Yesterday, 10:01 PM

LANDBANK

Dear Valued Client,

This is to inform you that you are attempting to transfer funds from your LandBank Savings Account :

Amount Transferred: Php 10,000.00
Bank Name:BDO Unibank
Destination Account: XXXXXXXXXX283



LANDBANK

Dear Valued Client,

This is to inform you that you are attempting to transfer funds from your LandBank Savings Account :

Amount Transferred: Php 10,000.00
Bank Name:BDO Unibank
Destination Account: XXXXXXXXXX283
Account Name:Andrea Angeles
Account Number: XXXXXXXXXX283
Convenience Fee:Php 25.00

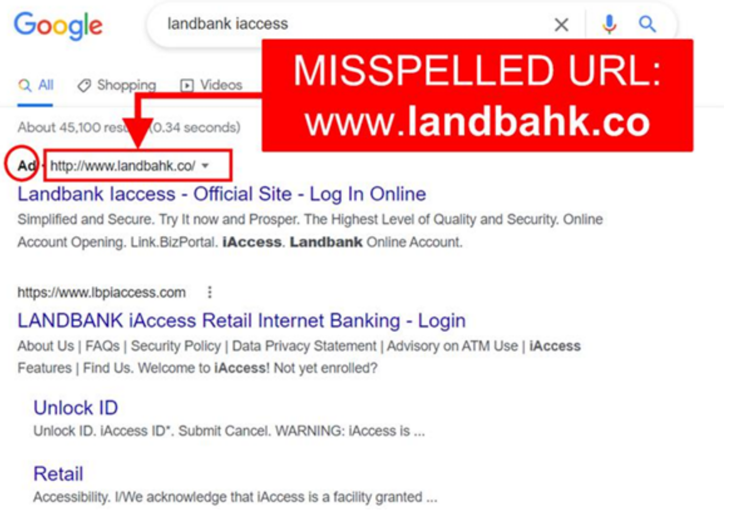
Make sure to double check your transaction to avoid encountering errors during transactions.

If you do not recognize this transaction, you may cancel the transaction

Click on the button below to continue.

Real-time Funds Transfer via instaPay

Several phishing websites purporting to be the website of Landbank iAccess are likewise appearing online. Below are some of the screenshots of the said phishing websites for reference:



Google

landbank iaccess

All · Shopping · Videos

MISSPELLED URL: www.landbahk.co

About 45,100 results (0.34 seconds)

Ad · http://www.landbahk.co/

Landbank Iaccess - Official Site - Log In Online

Simplified and Secure. Try It now and Prosper. The Highest Level of Quality and Security. Online Account Opening. Link.BizPortal. **iAccess**. **Landbank** Online Account.

https://www.lbpiaccess.com

LANDBANK iAccess Retail Internet Banking - Login

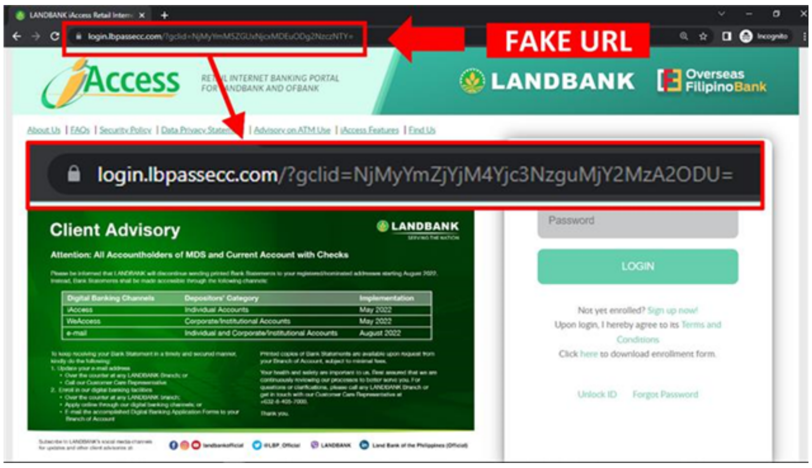
About Us | FAQs | Security Policy | Data Privacy Statement | Advisory on ATM Use | **iAccess** Features | Find Us. Welcome to **iAccess**! Not yet enrolled?

Unlock ID

Unlock ID. iAccess ID*. Submit Cancel. WARNING: iAccess is ...

Retail

Accessibility. I/We acknowledge that iAccess is a facility granted ...



LANDBANK iAccess Retail Intern

login.lbpassecc.com/?gclid=NjMyYmMSZGUxNjcxMDEuODg2NzczNTY=

FAKE URL

iAccess RETAIL INTERNET BANKING PORTAL FOR LANDBANK AND OFBANK

LANDBANK · Overseas Filipino Bank

About Us | FAQs | Security Policy | Data Privacy Statement | Advisory on ATM Use | iAccess Features | Find Us

login.lbpassecc.com/?gclid=NjMyYmZjYjM4Yjc3NzguMjY2MzA2ODU=

Client Advisory

Attention: All Accountholders of MDS and Current Account with Checks

Please be informed that LANDBANK will discontinue sending printed Bank Statements to your registered/nominated addresses starting August 2022. Instead, Bank Statements shall be made accessible through the following channels:

Digital Banking Channels	Depositors' Category	Implementation
iAccess	Individual Accounts	May 2022
WeAccess	Corporate/Institutional Accounts	May 2022
e-mail	Individual and Corporate/Institutional Accounts	August 2022

To keep receiving your Bank Statement in a timely and secured manner, kindly do the following:

1. Update your e-mail address
   - Over the counter at any LANDBANK Branch; or
   - Call our Customer Care Representative
2. Enroll in our digital banking facilities
   - Over the counter at any LANDBANK branch;
   - Apply online through our digital banking channels; or
   - E-mail the accomplished Digital Banking Application Form to your Branch of Account

Printed copies of Bank Statements are available upon request from your Branch of Account, subject to minimal fees.

Your health and safety are important to us. Rest assured that we are continuously reviewing our processes to better serve you. For questions or clarifications, please call any LANDBANK Branch or get in touch with our Customer Care Representative at +632-8-405-7000.

Thank you.

Subscribe to LANDBANK's social media channels for updates and other client advisories at: landbankofficial · @LBP_Official · LANDBANK · Land Bank of the Philippines (Official)

Password

LOGIN

Not yet enrolled? Sign up now!
Upon login, I hereby agree to its Terms and Conditions
Click here to download enrollment form.

Unlock ID · Forgot Password

The Official Landbank websites and email addresses are:

Landbank Sites:

https://www.lbpiaccess.com/

www.landbank.com

Landbank Email:

lbpmobileapps@mail.landbank.com
lbpiaccess@mail.landbank.com
customercare@mail.landbank.com**.**

Please immediately contact the LANDBANK Customer Care Hotline at (+632) 8-405-7000, PLDT Domestic Toll-Free Hotline at 1-800-10-405-7000, or email at customercare@mail.landbank.com if you have been a victim of phishing.

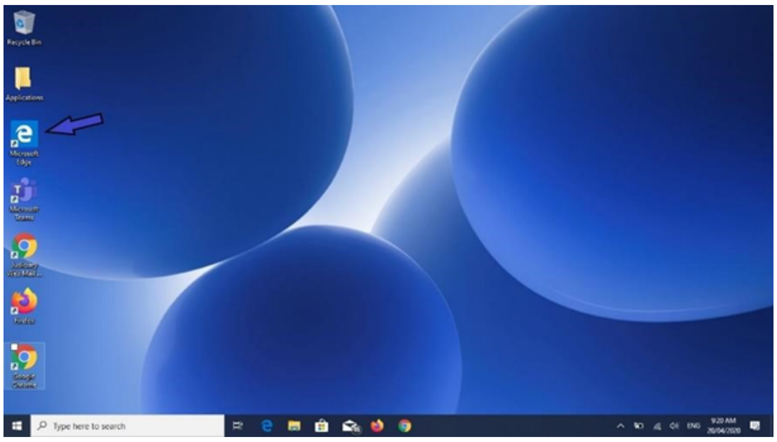
You may also contact the Management Information Systems Office (MISO) at support.email@judiciary.gov.ph for any assistance.

For your information and guidance.

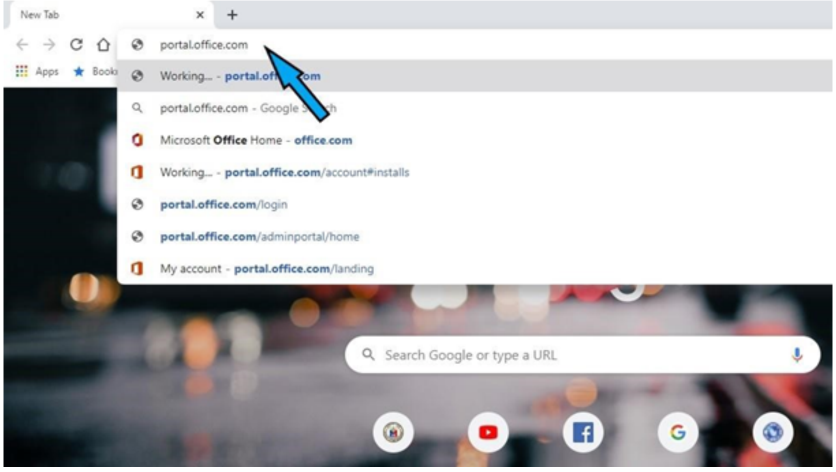
ANNEX B-1

INSTRUCTIONS FOR REGISTERING YOUR MULTI-FACTOR AUTHENTICATION FOR PHILIPPINE JUDICIARY 365 (PJ365)

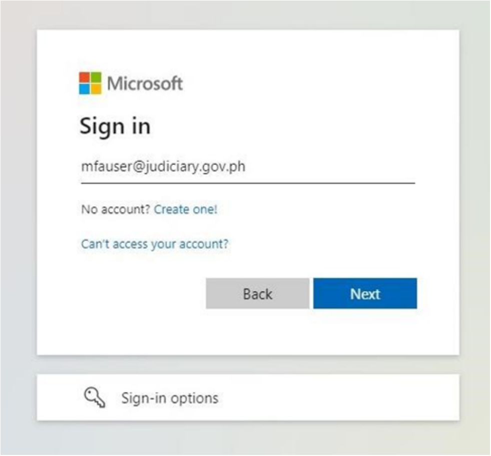
1. On your desktop computer, open your internet browser (i.e., Microsoft Edge, Google Chrome, Mozilla Firefox).



2. On the address bar, type *portal.office.com* and press Enter.


New Tab
Apps
Books
portal.office.com
Working... - portal.office.com
portal.office.com - Google Search
Microsoft Office Home - office.com
Working... - portal.office.com/account#installs
portal.office.com/login
portal.office.com/adminportal/home
My account - portal.office.com/landing
Search Google or type a URL

3. In the sign-in box, type your PJ365 email address (e.g., user@judiciary.gov.ph) and click *Next*.


Microsoft

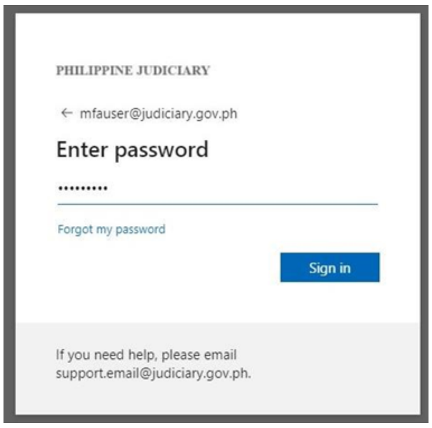
Sign in

mfauser@judiciary.gov.ph

No account? Create one!

Can't access your account?

4. Type in your assigned password and click the *Sign in* button.



PHILIPPINE JUDICIARY

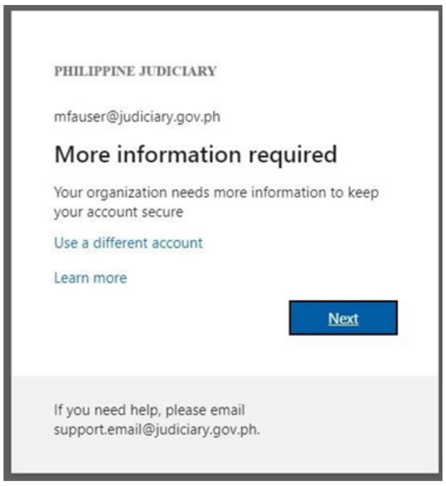
← mfauser@judiciary.gov.ph

Enter password

•••••••••

If you need help, please email support.email@judiciary.gov.ph.

5. A new window requiring more information will appear. Click *Next***.**



PHILIPPINE JUDICIARY

mfauser@judiciary.gov.ph

More information required

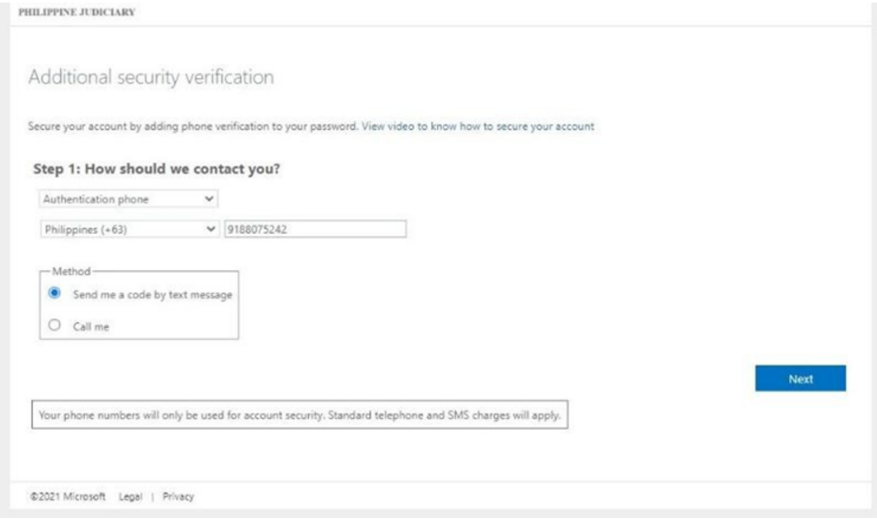
Your organization needs more information to keep your account secure

If you need help, please email support.email@judiciary.gov.ph.

6. You will then be required to choose which authentication method you would like to enroll for your account.

MOBILE PHONE AS AUTHENTICATION METHOD

a. Choose **Authentication phone** as the default authentication method. Input your mobile number, select **Send me a code by text message**, and click **Next.**



PHILIPPINE JUDICIARY

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Authentication phone

Philippines (+63) 9188075242

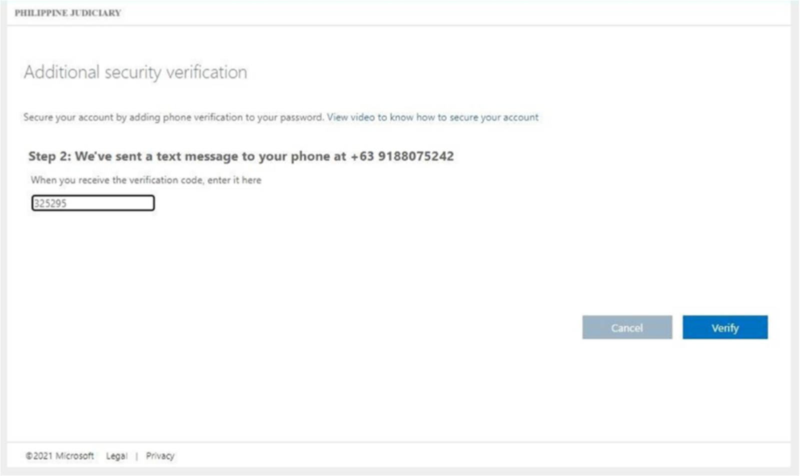
Method

● Send me a code by text message

○ Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

b. You will then receive a text message from Microsoft containing the 6-digit code for verification. Enter the code and press *Verify*.



PHILIPPINE JUDICIARY

Additional security verification

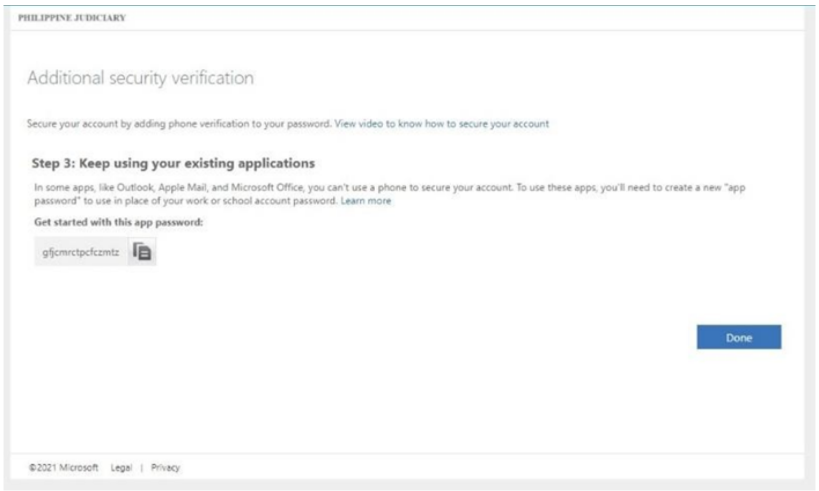
Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 2: We've sent a text message to your phone at +63 9188075242

When you receive the verification code, enter it here

325295

c. To finish setup, click Done.



PHILIPPINE JUDICIARY

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

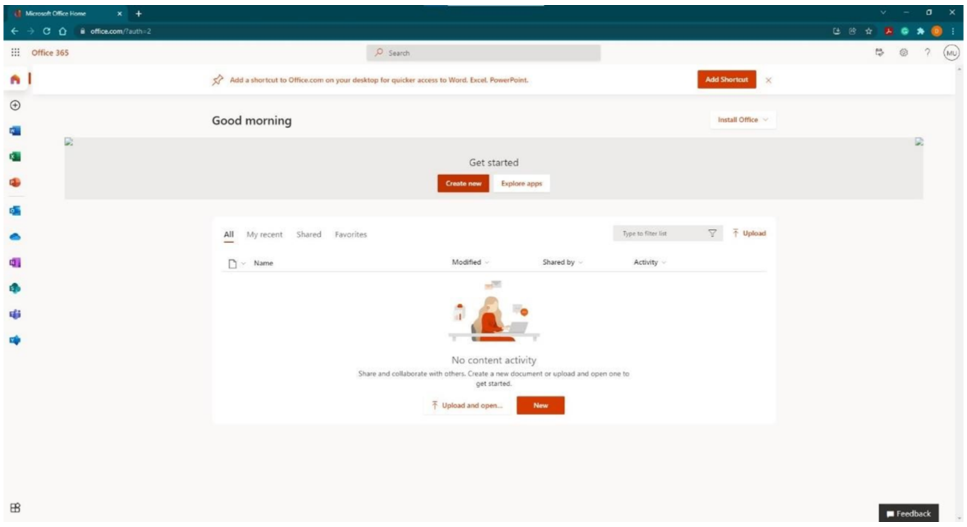
Step 3: Keep using your existing applications

In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. Learn more

Get started with this app password:

gfjcmrctpcfczmtz

d. You will now be redirected to the welcome screen of your Office 365 account.



Add a shortcut to Office.com on your desktop for quicker access to Word. Excel. PowerPoint.

Good morning

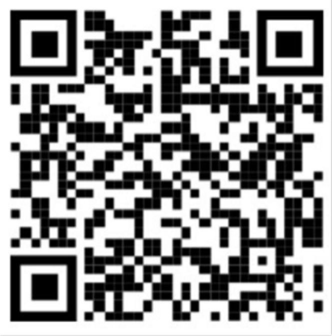
No content activity

Share and collaborate with others. Create a new document or upload and open one to get started.

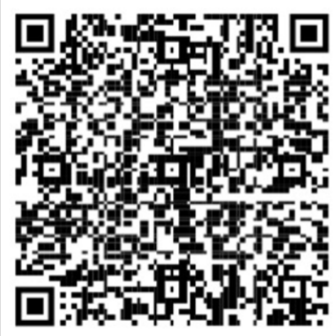
HOW TO ENROLL YOUR ACCOUNT TO THE MICROSOFT AUTHENTICATOR APP MOBILE FOR ANDROID AND IOS

1. On your mobile phone, install **Microsoft Authenticator**. You can download this application through the App Store for Apple devices or Google Play for Android devices. You can also scan the QR code below

App Store



Google Play



2. Once you have installed **Microsoft Authenticator** on your device, open the application and choose **Add account** (See ***Fig. 1***) > choose **Work or school account** (See ***Fig. 2***) > accept the required app permissions > choose **Sign in** (*See* ***Fig 3***).

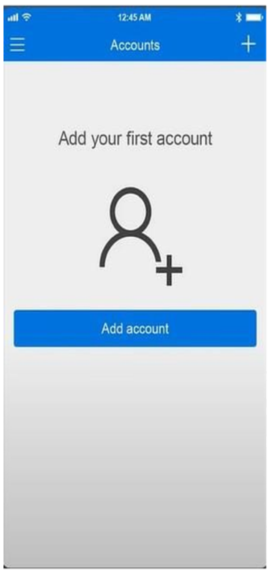


Fig 1

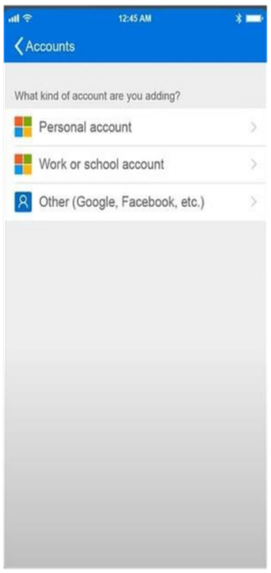

12:45 AM
Accounts
What kind of account are you adding?
Personal account
Work or school account
Other (Google, Facebook, etc.)

Fig 2

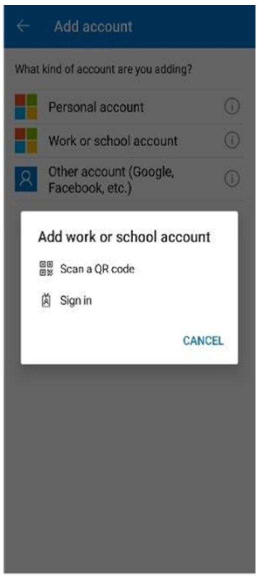
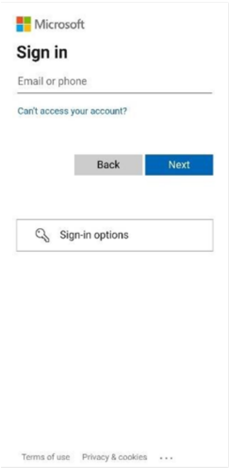

Add account
What kind of account are you adding?
Personal account
Work or school account
Other account (Google, Facebook, etc.)
Add work or school account
Scan a QR code
Sign in
CANCEL

Fig 3

3. In the PJ365 sign-in dashboard (See Fig. 4)
    a. Enter your password (See Fig. 5)
    b. Choose text to verify your identity (See Fig. 6)
    c. Enter the six-digit number (See Fig. 7)


Microsoft

Sign in

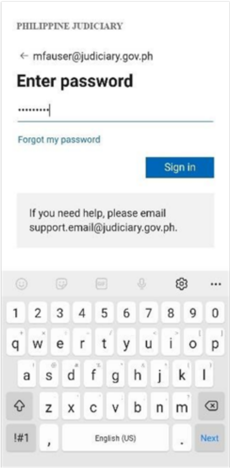
Email or phone

Can't access your account?

Back Next

Sign-in options

Fig 4


PHILIPPINE JUDICIARY

← mfauser@judiciary.gov.ph

Enter password

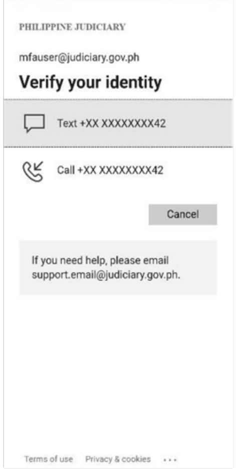
••••••••

Forgot my password

Sign in

If you need help, please email support.email@judiciary.gov.ph.

Fig 5


PHILIPPINE JUDICIARY

mfauser@judiciary.gov.ph

Verify your identity

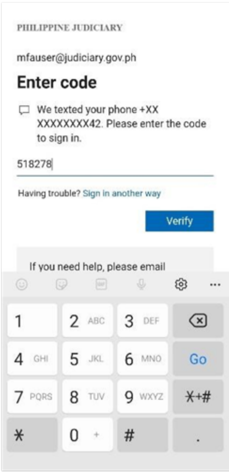
Text +XX XXXXXXXX42

Call +XX XXXXXXXX42

Cancel

If you need help, please email support.email@judiciary.gov.ph.

Fig 6


PHILIPPINE JUDICIARY

mfauser@judiciary.gov.ph

Enter code

We texted your phone +XX XXXXXXXX42. Please enter the code to sign in.

518278

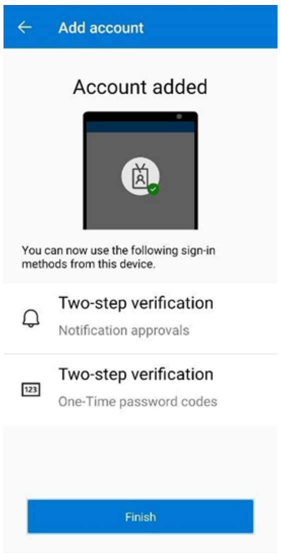
Having trouble? Sign in another way

Verify

If you need help, please email

Fig 7

4. Click **Finish** to complete your setup.


← Add account

Account added

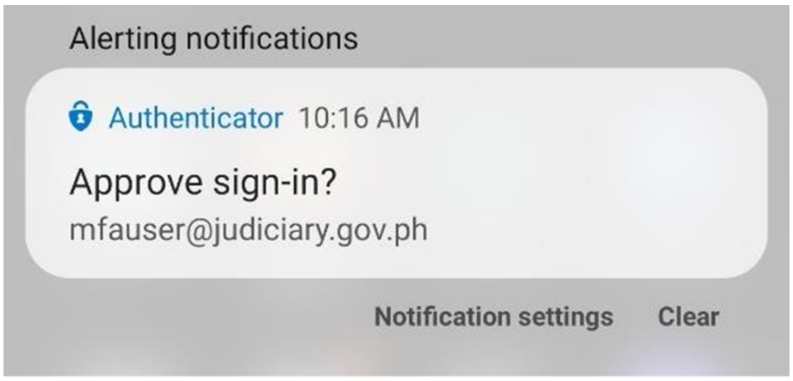
You can now use the following sign-in methods from this device.

Two-step verification
Notification approvals

Two-step verification
One-Time password codes

Finish

5. You will have the option to **Deny** or **Approve** the account sign-in.


Alerting notifications

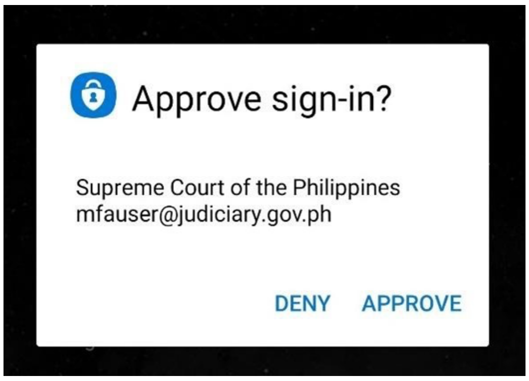
Authenticator 10:16 AM

Approve sign-in?

mfauser@judiciary.gov.ph

Notification settings Clear

6. For future sign-ins, you should receive a notification from the Microsoft Authenticator app for confirmation – to either approve or deny the sign-in.



Approve sign-in?

Supreme Court of the Philippines
mfauser@judiciary.gov.ph

Please follow the guidelines below for creating a strong password.

A Strong Password should:

1. be at least 12 characters in length
2. contain both upper and lowercase alphabetic characters (e.g., A-Z, a-z)
3. have at least one numerical character (e.g., 0-9)
4. have at least one special character (e.g. ~!@#$%^&*()_-+=)

A Strong Password should not:

1. spell a word or series of words that can be found in a standard dictionary
2. spell a word with a number added to the beginning and the end
3. be based on any personal information such as user id, family name, pet, birthday, etc.

A strong password is one that is easy for you to remember but difficult for others to guess. Below are some of the most important things to remember when creating a password:

1. **Never use personal information such as your name, birthday, username, or email address.** This type of information is often publicly available, which makes it easier for someone to guess your password.
2. **Use a longer password.** Your password should be at least twelve (12) characters long, which contains numbers, symbols, and both uppercase and lowercase letters.
3. These tips can help you create strong passwords that are easier to remember. Try to use:
    1. A lyric from a song or poem
    2. A meaningful quote from a movie or speech
    3. A passage from a book
    4. A series of words that are meaningful to you
    5. An abbreviation: Make a password from the first letter of each word in a sentence
4. Avoid choosing passwords that could be guessed by:
    1. People who know you
    2. People looking at easily accessible info (like your social media profile)
5. **Don't use the same password for each account.** If someone discovers your password for one account, all of your other accounts will be vulnerable.
6. **Avoid using words that can be found in the dictionary.** For example, justice123 would be a weak password.

7. Random passwords or passphrases are the strongest.
8. Once you’ve chosen a strong password, you can protect it by following the simple rules below: ▪ Don’t share your password with anyone.
    1. Never give your password to people who call you on the phone or send unsolicited email, even if they claim to be from the MISO.
    2. If you have trouble remembering multiple passwords, consider using a trusted password manager. Take some time to research the reviews and reputations of these services.
    3. If you need to write your password down, don’t leave it on your computer or desk. Make sure any written passwords are stored somewhere that is secured.

ANNEX B-2

HOW TWO-FACTOR AUTHENTICATION WORKS ON FACEBOOK

Two-factor authentication is a security feature that helps protect your Facebook account in addition to your password. If you set up two-factor authentication, you'll be asked to enter a special login code or confirm your login attempt each time someone tries accessing Facebook from a browser or mobile device we don't recognize. You can also get alerts when someone tries logging in from a browser or mobile device we don't recognize.

Turn on or manage two-factor authentication

1. Go to your Security and Login Settings.
2. Scroll down to **Use two-factor authentication** and click **Edit**.
3. Choose the security method you want to add and follow the on-screen instructions.

When you set up two-factor authentication on Facebook, you'll be asked to choose one of three security methods:

- Tapping your security key on a compatible device.
- Login codes from a third-party authentication app.
- Text message (SMS) codes from your mobile phone.

Once you've turned on two-factor authentication, you can get 10 recovery login codes to use when you're unable to use your phone. Learn how to set up recovery codes.

Other Useful Resources

- If you haven't saved the browser or mobile device you're using, you'll be asked to do so when you turn on two-factor authentication. This way you won't have to enter a security code when you log in again. Don't click **Save this browser** if you're using a public computer that other people can access (example: a library computer).
- We need to be able to remember your computer and browser information so we can recognize it the next time you log in. Some browser features block this. If you've turned on private browsing or set up your browser to clear your history every time it closes, you might have to enter a code every time you log in.
- To set up text message (SMS) two-factor authentication, you can either use a mobile number that's already been added to your account or add a new number.
- Learn about what you can do if you turned on two-factor authentication but are now having trouble logging in.

REFERENCE

https://www.facebook.com/help/148233965247823?helpref=search&query=two%20factor%20authentication&search_session_id=f91cf9a5c6bf78b99dbd3c0999440297&sr=3

ANNEX B-3

HOW TO TURN INSTAGRAM TWO-FACTOR AUTHENTICATION FOR MULTIPLE DEVICES ON OR OFF

To set up two-factor authentication on additional devices:

1. Click **More** in the bottom left, then click **Settings**.
2. Click **Accounts Center**.
3. Click **Password and security** then select **Two-factor authentication**.
4. Click **Authentication app**, then click **Copy key** or use the QR code to link your account to the authentication app.
5. After your Instagram account is linked to your authentication app, copy the 6-digit code your authentication app creates.
6. Go back to Instagram on your computer, click **Next** and paste the 6-digit code to complete the process on that device.

Keep in mind that you can add up to five connected devices to two-factor authentication for a single Instagram account and you can remove a connected device at any time.

Your Instagram key can also be used if you use multiple authentication apps on the same device. To do this, follow the steps above on the same device.

To remove a connected device from two-factor authentication:

1. Click **More** in the bottom left, then click **Settings**.
2. Click **Accounts Center**.
3. Click **Password and security** then select **Two-factor authentication**.
4. Click **Instagram**, then select the method you are using to get login codes (example: text message, WhatsApp, or authentication app).
5. Click **Turn off**.

Removing a connected device from two-factor authentication does not log it out from your account.

REFERENCE

https://help.instagram.com/1124604297705184

ANNEX B-4

GOOGLE MULTIFACTOR AUTHENTICATION

Turn on 2-Step Verification

With 2-Step Verification, also called two-factor authentication, you can add an extra layer of security to your account in case your password is stolen. After you set up 2-Step Verification, you can sign into your account with:

- Your password
- Your phone

Allow 2-Step Verification

2. Open your Google Account.
3. In the navigation panel, select **Security**.
4. Under “Signing into Google,” select **2-Step Verification Get started**.
5. Follow the on-screen steps.

Tip: If you use an account through your work, school, or other group, these steps might not work. If you can’t set up 2-Step Verification, contact your administrator for help.

Verify it’s you with a second step

After you turn on 2-Step Verification, you must complete a second step to verify it’s you when you sign in. To help protect your account, Google will ask that you complete a specific second step.

Computer Android iPhone & iPad

Use Google prompts

We recommend you sign in with Google prompts. It's easier to tap a prompt than enter a verification code. Prompts can also help protect against SIM swap and other phone number-based hacks.

Google prompts are push notifications you’ll receive on:

- Android phones that are signed into your Google Account.
- iPhones with the Smart Lock app, the Gmail app, the Google Photos app, the YouTube app, or Google app signed in to your Google Account.

Based on the device and location info in the notification, you can:

- Allow the sign in if you requested it by tapping **Yes**
- Block the sign-in if you didn’t request it by tapping **No**

For added security, Google may ask you for your PIN or other confirmation.

Use other verification methods

You can set up other verification methods in case you:

- Want increased protection against phishing
- Can’t get Google prompts
- Lose your phone

https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform=Desktop

ANNEX C

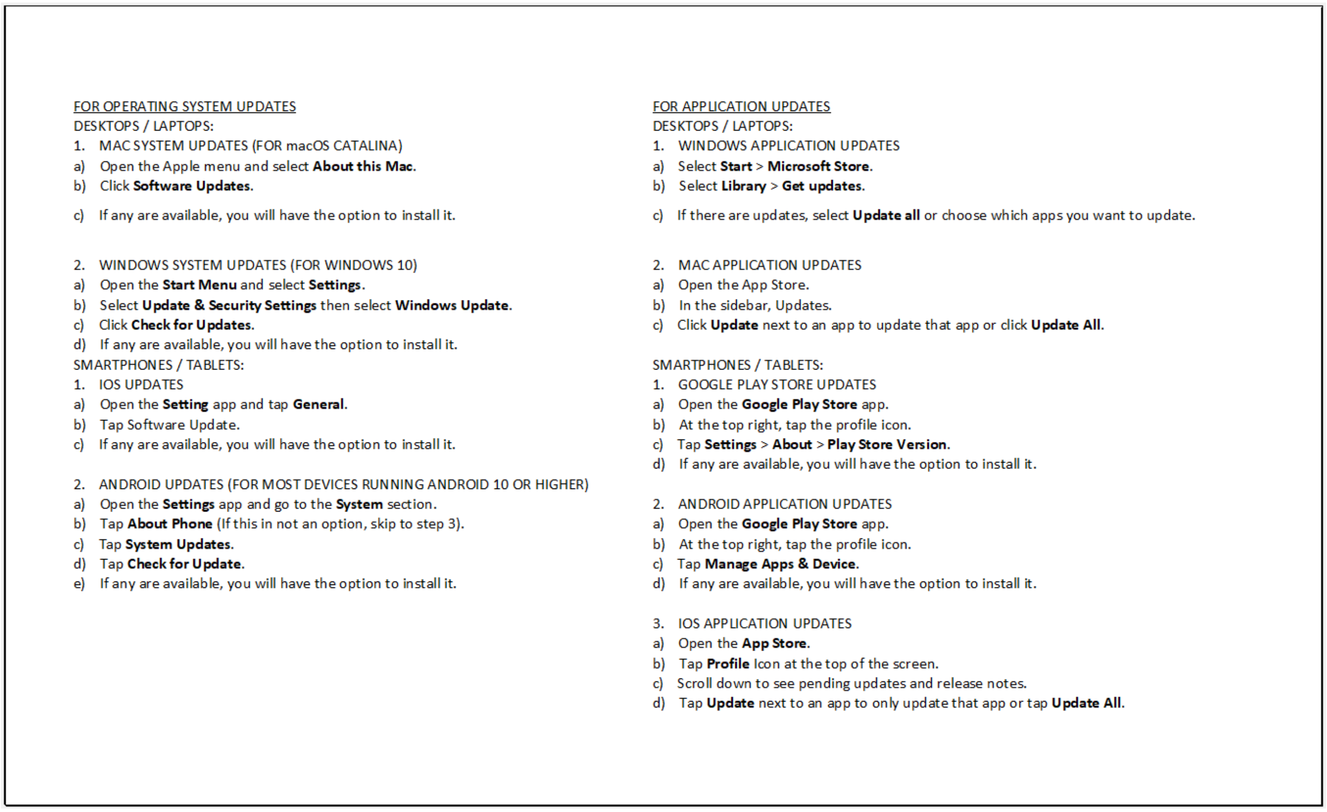
CYBERSECURITY ADVISORY NO. 2022-04

Microsoft August 2022 Patch Tuesday fixes exploited zero-day vulnerabilities

We respectfully advise all magistrates, court officials and employees to keep the software of your devices up to date by running the update functionality on a regular basis. Repeatedly delaying software updates despite receiving multiple prompts may lead to security risks that can make devices susceptible to malware, viruses, and zero-day vulnerabilities.

A zero-day vulnerability is a flaw, weakness, or bug in a software, firmware, or hardware that has become discovered by attackers prior to the discovery of the vendor. Since vendors are unaware of its existence, the vulnerability remains unpatched, making attacks more likely to succeed. Software patches are regularly deployed as soon as possible for newly discovered system vulnerabilities. While this cannot prevent zero-day attacks, quickly applying patches and software upgrades can significantly reduce the risk of an attack.

In view thereof, the following steps should be undertaken to update your respective devices:



FOR OPERATING SYSTEM UPDATES

DESKTOPS / LAPTOPS:

1. MAC SYSTEM UPDATES (FOR macOS CATALINA)

a) Open the Apple menu and select **About this Mac.**
b) Click **Software Updates.**
c) If any are available, you will have the option to install it.

2. WINDOWS SYSTEM UPDATES (FOR WINDOWS 10)

a) Open the **Start Menu** and select **Settings.**
b) Select **Update & Security Settings** then select **Windows Update.**
c) Click **Check for Updates.**
d) If any are available, you will have the option to install it.

SMARTPHONES / TABLETS:

1. IOS UPDATES

a) Open the **Setting** app and tap **General.**
b) Tap Software Update.
c) If any are available, you will have the option to install it.

2. ANDROID UPDATES (FOR MOST DEVICES RUNNING ANDROID 10 OR HIGHER)

a) Open the **Settings** app and go to the **System** section.
b) Tap **About Phone** (If this in not an option, skip to step 3).
c) Tap **System Updates.**
d) Tap **Check for Update.**
e) If any are available, you will have the option to install it.

FOR APPLICATION UPDATES

DESKTOPS / LAPTOPS:

1. WINDOWS APPLICATION UPDATES

a) Select **Start** > **Microsoft Store.**
b) Select **Library** > **Get updates.**
c) If there are updates, select **Update all** or choose which apps you want to update.

2. MAC APPLICATION UPDATES

a) Open the App Store.
b) In the sidebar, Updates.
c) Click **Update** next to an app to update that app or click **Update All.**

SMARTPHONES / TABLETS:

1. GOOGLE PLAY STORE UPDATES

a) Open the **Google Play Store** app.
b) At the top right, tap the profile icon.
c) Tap **Settings** > **About** > **Play Store Version.**
d) If any are available, you will have the option to install it.

2. ANDROID APPLICATION UPDATES

a) Open the **Google Play Store** app.
b) At the top right, tap the profile icon.
c) Tap **Manage Apps & Device.**
d) If any are available, you will have the option to install it.

3. IOS APPLICATION UPDATES

a) Open the **App Store.**
b) Tap **Profile** Icon at the top of the screen.
c) Scroll down to see pending updates and release notes.
d) Tap **Update** next to an app to only update that app or tap **Update All.**

The Management Information Systems Office (MISO) may be reached at miso.sc@judiciary.gov.ph for any assistance.

Please be guided accordingly.

Thank you.