

# Wiki

Informasi tentang Wiki ini.

- [MBF IT Support](#)
- [HDD vs SSD untuk PC .. lebih baik pakai yang mana?](#)
- [Peningkatan Kesadaran dan Pencegahan Serangan Ransomware dan Virus](#)
- [Pengoperasian TV Ruang Meeting](#)
- [WhatsApp anda kena retas?](#)
- [PWA \(Progressive Web App\) dan panduan cara Instalasinya di iOS dan Android.](#)
- [Modus Baru Bobol M-Banking Kuras Rekening Muncul di RI Jelang Lebaran](#)

# MBF IT Support

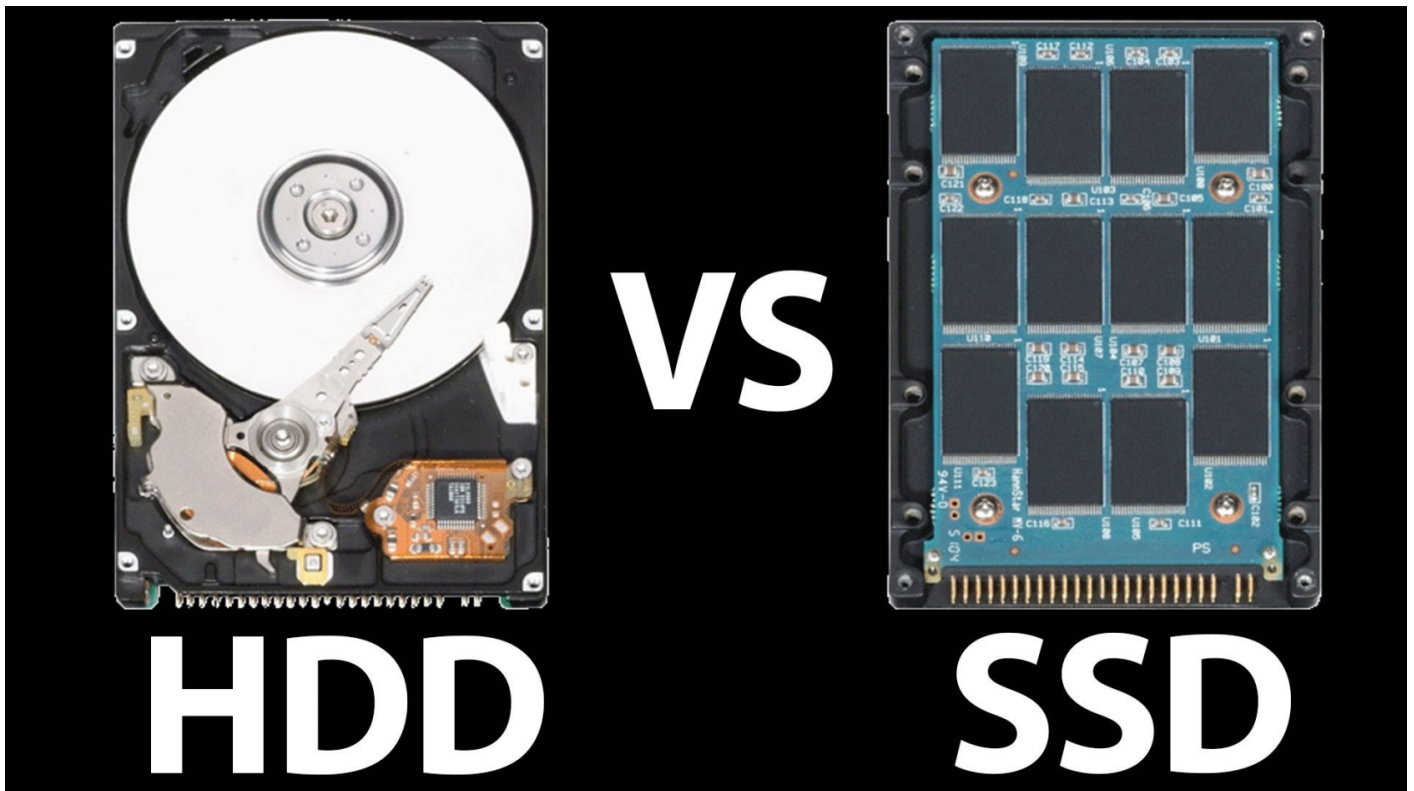
Staff IT yang akan Standby pukul 16.30 s/d 17.30 WIB pada Minggu ini :

Hari	Nama	Ext
Senin	Ibrahim	241
Selasa	Hendar	241
Rabu	Hermin	242
Kamis	Ridho	244
Jumat	Eko	253

IT Support

# HDD vs SSD untuk PC .. lebih baik pakai yang mana?

14 Februari 2025, IT Infra



Mari kita bahas perbandingan antara HDD (Hard Disk Drive) dan SSD (Solid State Drive) untuk kebutuhan PC/Laptop kantor:

## HDD (Hard Disk Drive)

### Kelebihan

- **Kapasitas Besar:** HDD menawarkan kapasitas penyimpanan yang lebih besar dengan harga yang lebih terjangkau. Ini ideal untuk menyimpan banyak dokumen, foto, video, dan file lainnya.
- **Harga Terjangkau:** Harga per gigabyte HDD lebih murah dibandingkan SSD, sehingga lebih ekonomis untuk kapasitas besar.

- **Umur Panjang:** HDD memiliki umur pakai yang cukup panjang jika digunakan dengan benar dan tidak mengalami kerusakan fisik.

## Kekurangan

- **Kecepatan Lebih Lambat:** Waktu akses dan transfer data HDD lebih lambat dibandingkan SSD karena menggunakan komponen mekanis yang bergerak. Ini dapat mempengaruhi kinerja komputer secara keseluruhan.
- **Rentan Terhadap Kerusakan:** Komponen mekanis pada HDD membuatnya lebih rentan terhadap kerusakan akibat benturan atau getaran. Ini bisa menjadi masalah jika Anda sering membawa-bawa laptop.
- **Lebih Berisik:** HDD menghasilkan suara yang lebih bising saat beroperasi karena adanya putaran piringan di dalamnya.
- **Lebih Berat dan Tebal:** HDD umumnya lebih berat dan tebal daripada SSD, yang dapat mempengaruhi portabilitas laptop secara keseluruhan.
- **Konsumsi Daya Lebih Tinggi:** HDD cenderung mengkonsumsi daya lebih besar dibandingkan SSD. Untuk laptop bisa jadi mengurangi daya tahan baterai.

## SSD (Solid State Drive)

### Kelebihan

- **Kecepatan Tinggi:** SSD menawarkan kecepatan akses dan transfer data yang jauh lebih cepat dibandingkan HDD. Ini membuat komputer booting lebih cepat, aplikasi terbuka lebih responsif, dan transfer file lebih cepat.
- **Lebih Tahan Lama:** SSD tidak memiliki komponen mekanis yang bergerak, sehingga lebih tahan terhadap benturan dan getaran. Ini sangat penting untuk laptop yang sering dibawa-bawa.
- **Lebih Senyap:** SSD beroperasi tanpa suara karena tidak ada bagian yang berputar.
- **Lebih Ringan dan Tipis:** SSD umumnya lebih ringan dan tipis daripada HDD, sehingga berkontribusi pada portabilitas laptop secara keseluruhan.
- **Konsumsi Daya Lebih Rendah:** SSD umumnya mengkonsumsi daya lebih sedikit dibandingkan HDD. Hal ini dapat membantu memperpanjang daya tahan baterai Laptop anda.

### Kekurangan

- **Harga Lebih Mahal:** Harga per gigabyte SSD lebih mahal dibandingkan HDD.
- **Kapasitas Lebih Kecil:** Kapasitas penyimpanan SSD biasanya lebih kecil dibandingkan HDD dengan harga yang sama.

- **Umur Pakai Terbatas:** Meskipun lebih tahan terhadap kerusakan fisik, SSD memiliki umur pakai terbatas karena sel-sel memori flash memiliki siklus baca/tulis yang terbatas.

# Kesimpulan

Untuk PC kantor, pilihan antara HDD dan SSD tergantung pada kebutuhan dan anggaran Anda.

- **Jika Anda membutuhkan kapasitas penyimpanan besar dengan harga terjangkau dan tidak terlalu mempermasalahkan kecepatan, HDD bisa menjadi pilihan yang baik.**
- **Jika Anda mengutamakan kecepatan dan kinerja komputer yang lebih baik, SSD adalah pilihan yang lebih disarankan, meskipun dengan harga yang lebih mahal.**

# Pertimbangan Tambahan

- **Hybrid Drive (SSHD):** Merupakan kombinasi antara HDD dan SSD. SSHD menawarkan kecepatan yang lebih baik dari HDD biasa dengan harga yang masih relatif terjangkau.
- **Dual Drive:** Anda juga dapat menggunakan kombinasi HDD dan SSD. SSD digunakan untuk sistem operasi dan aplikasi yang sering digunakan, sedangkan HDD digunakan untuk menyimpan data yang lebih besar.

Semoga informasi ini bermanfaat!

# Peningkatan Kesadaran dan Pencegahan Serangan Ransomware dan Virus

Versi Video:

Klik pada video untuk memulai. Double-click untuk memperbesar tampilan video. Tersedia suara narator dan caption.

Versi Teks:

Yth. Bapak/Ibu,

Akhir-akhir ini, serangan virus dan ransomware yang menyasar perusahaan dan institusi, baik swasta maupun pemerintah, kembali marak terjadi. Sebagai contoh, serangan ransomware baru-baru ini menimpa server PDN (Pusat Data Nasional) di lingkungan KOMINFO (Kementerian Komunikasi dan Informatika) dengan varian ransomware Brain Cipher.

Apa itu ransomware dan Brain Cipher Ransomware?

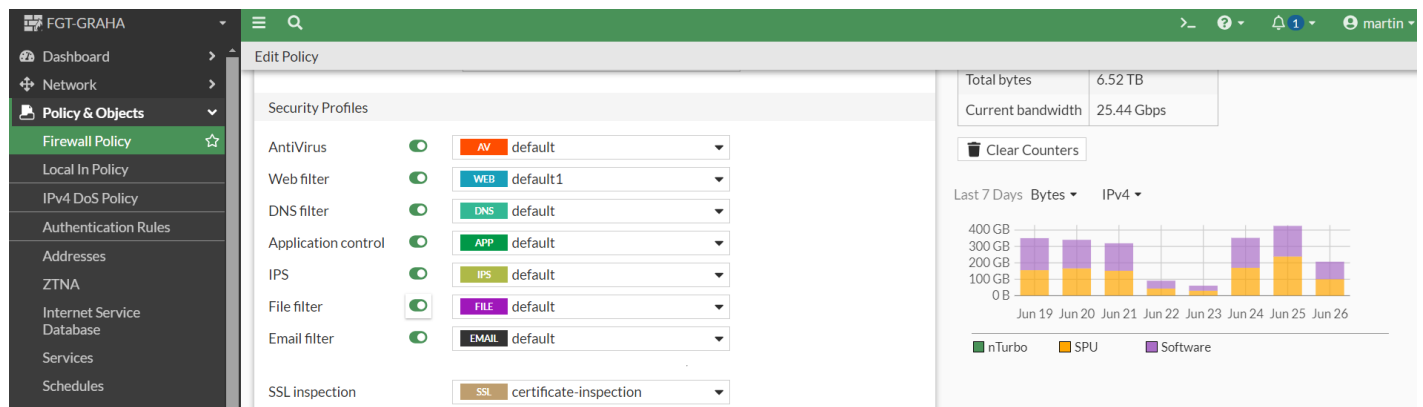
Ransomware adalah jenis malware yang digunakan peretas untuk menyandera data penting milik korban, baik individu maupun korporasi, dengan mengenkripsi data tersebut. Pelaku kemudian akan meminta tebusan berupa uang, termasuk cryptocurrency seperti Bitcoin.

a. Brain Cipher Ransomware adalah geng peretas yang menggunakan varian ransomware Lockbit untuk menyerang sistem korban, menurut Broadcom, penyedia layanan keamanan siber Symantec. Informasi lebih lanjut dapat ditemukan di <https://kumparan.com/kumparantech/apa-itu-brain-cipher-ransomware-yang-bikin-lumpuh-server-pdn-kominfo-2302QtPRjyx/4> .

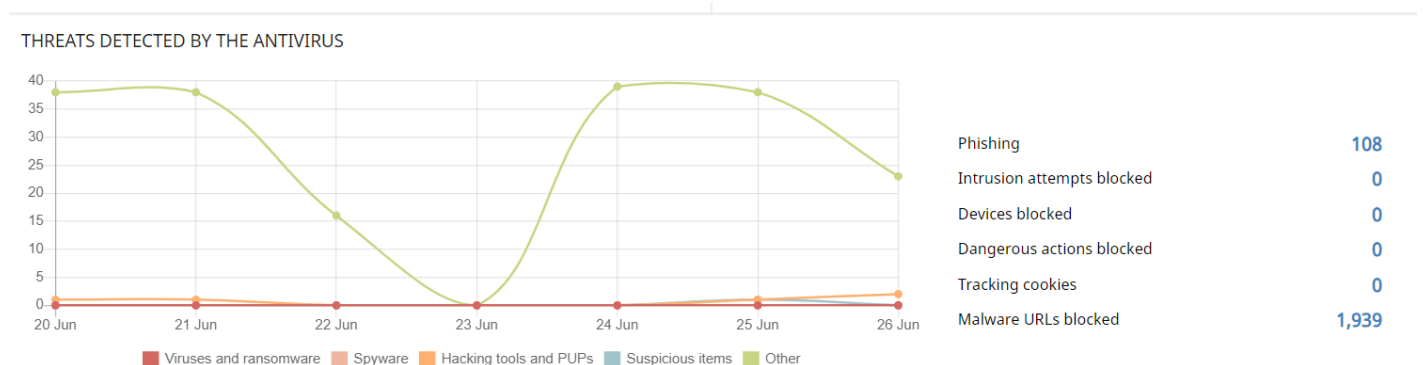
b. Brain Cipher Ransomware adalah jenis ransomware baru yang muncul tahun ini. Ransomware ini mengenkripsi file korban dan meminta tebusan sebagai ganti kunci dekripsi. Peretas biasanya menyebarkan email phishing atau unduhan berbahaya, mengeksploitasi kerentanan dalam sistem untuk mendapatkan akses. Serangan ini menggunakan teknik canggih untuk menyusup, menyebar, dan mengenkripsi data dalam jaringan yang ditargetkan. Metode pengiriman utamanya adalah melalui email phishing, yang sering kali berisi lampiran atau tautan berbahaya yang mengarah ke unduhan malware. Informasi lebih lanjut dapat ditemukan di <https://katadata.co.id/digital/teknologi/66796641b9261/apa-itu-brain-cipher-ransomware-yang-serang-pusat-data-nasional> .

Untuk mencegah serangan ransomware dan virus lainnya, langkah-langkah yang telah diterapkan di lingkungan MBF meliputi peningkatan keamanan jaringan yang berlapis dengan menggunakan firewall dan antivirus.

1. **Firewall:** Penggunaan firewall diterapkan mulai dari masuknya koneksi internet ISP yang difilter perangkat firewall untuk menyaring data masuk mulai dari antivirus, web, aplikasi, file, sampai email filter.



2. **Antivirus:** Di layer end-user, selain antivirus layer jaringan, MBF juga menggunakan antivirus yang diinstal di PC dan laptop. Antivirus ini mendeteksi virus, ransomware, spyware, hacking tools, dan Potentially Unwanted Programs (PUP).



3. **Backup Data:** Backup data server dilakukan secara periodik. Backup data dari server produksi, database, email, web, dan file server disimpan di server Linux yang lebih aman dari serangan virus.

Veeam Backup and Replication

Home View Job

Start Stop Retry Active Full Statistics Report Edit Clone Disable Delete

Job Control Details Manage Job

Home

Jobs

- Backup
- Backup Copy
- Backups
- Disk
- Disk (Copy)
- Last 24 Hours
- Success

Home

Inventory

- Backup Infrastructure
- Storage Infrastructure
- Tape Infrastructure

Type in an object name to search for

All jobs

Name	Type	Objects	Status	Last Run	Last Result
App LIVE Daily 1X HRIS App	Windows Agent Backup	1	Stopped	12 hours ago	Success
App LIVE Daily 1X IA-FOXPRO	Windows Agent Backup	1	Stopped	12 hours ago	Success
App LIVE Daily 1X IA-Web App & DB	Windows Agent Backup	1	Stopped	12 hours ago	Success
App LIVE Daily 1X Web App	Windows Agent Backup	1	Stopped	12 hours ago	Success
Backup Copy	Backup Copy	20	Stopped	19 minutes ago	Success
DB LIVE Daily 2X - Navision	Windows Agent Backup	1	Stopped	1 hour ago	Success
DB LIVE Daily 3X HRIS	Windows Agent Backup	1	Stopped	1 hour ago	Success
DB LIVE Daily 3X L2/L3	Windows Agent Backup	1	Stopped	27 minutes ago	Success
DB LIVE Daily 3X Web	Windows Agent Backup	1	Stopped	58 minutes ago	Success
Linux Web Server Daily Backup	Linux Agent Backup	1	Stopped	10 hours ago	Success
NAS Server LIVE Daily 2X NAS-2 Graha	Windows Agent Backup	1	Stopped	31 minutes ago	Success
NAS Server LIVE Daily 2X NAS-5 Plant	Windows Agent Backup	1	Stopped	26 minutes ago	Success
TOOLS - Daily 1X IA Active Directory	Windows Agent Backup	1	Stopped	14 hours ago	Success
TOOLS - Daily 1X MBF Active Directory	Windows Agent Backup	1	Stopped	14 hours ago	Success

SUMMARY

Duration: 04:34

Processing rate: 12 GB/s

Bottleneck: N/A

DATA

Processed: 3.1 TB (100%)

Read: 0 B

Transferred: 0 B

STATUS

Success: 1

Warnings: 0

Errors: 0

THROUGH

id: 0 KB


Namun demikian, selain semua usaha preventif yang sudah dilakukan, kami juga mengharapkan peran serta dari seluruh user MBF untuk selalu waspada dan berhati-hati, terutama ketika menggunakan jaringan internet di kantor. Hindari mengakses atau membuka link yang diperoleh dari web atau email secara sembarangan. Jika membawa flash disk dari luar, harap selalu melakukan pemindaian terlebih dahulu.

Khusus untuk email, jika menerima email, jangan sembarang membuka lampiran atau mengklik link atau tombol yang ada di dalam email tersebut. Banyak email yang tampak valid tetapi sebenarnya mengandung virus dan link ransomware. Jika menerima email yang mencurigakan, harap segera menghapusnya dan jangan mengklik tautan yang ada di dalam email tersebut. Apabila ragu, silakan menanyakan terlebih dahulu ke IT Support.



## Action is Required on martin.widjaja@mbf.co.i...



From **cPanel E-mail Administrator**   
To **martin.widjaja@md@nti.edu.pk**  
Date **2024-06-11 06:54**

Arahkan kursor pada Nama,  
nanti muncul alamat email  
pengirim, TIDAK DIKENAL

Sent from a trusted sender.

Walaupun ada kata-kata ini.

Hello **martin.widjaja@mbf.co.id**,

You have 14 emails pending.

Follow the link below to release it all to your inbox.

**RELEASE NOW**

Regards

Jangan pernah klik tombol atau link pada email yang mencurigakan

**mbf.co.id cPanel Security Gateway**

This is a service notification and does not mean you will receive mass mailings from us.

This message is auto-generated from Drakephilippines Security Gateway; replies sent to this email cannot be delivered.

Copyright © 2024 Inc. All rights reserved

Mari kita bersama-sama peduli, teliti, disiplin, dan saling menjaga terkait data perusahaan.

Demikian himbauan dan informasi dari kami. Jika masih belum paham, jangan sungkan untuk bertanya ke Tim IT Support.

# Pengoperasian TV Ruang Meeting

Pada beberapa ruang meeting, sudah disediakan Samsung Smart TV sebagai pengganti proyektor, yaitu :

1. Ruang Meeting Brantas (Lantai 1)
2. Ruang Meeting Musi (Lantai 1)
3. Ruang Meeting Kapuas (Lantai 2)
4. Ruang Meeting Asahan (Lantai 2 - by DMA)

Cara menggunakannya ada beberapa metode:

## Metode Wireless Display

Laptop dengan sistem operasi Windows 10 atau terbaru, sudah dapat terhubung langsung dengan TV tanpa menggunakan kabel HDMI, caranya:

1. Pastikan Laptop sudah terhubung ke WiFi MBF atau DMA
  - untuk Ruang Meeting Musi dan Brantas di Graha gunakan MBF-MGR
  - untuk Ruang Meeting Kapuas dan Asahan di Graha bisa menggunakan MBF-AP
  - untuk Ruang Meeting Mahakam di Plant bisa menggunakan MBF-AP-5G atau MBF-MAHAKAM
2. Hidupkan Samsung Smart TV
3. Pada Laptop, tekan secara bersamaan tombol Windows dan Keyboard huruf K (⊞+ K) , maka akan muncul menu Casting seperti pada gambar dibawah ini.
4. Selanjutnya akan muncul pilihan Samsung Smart TV yang ada di jaringan, klik sesuai dengan ruang meeting yang sedang anda gunakan.
  - TV85Brantas
  - TV75Musi
  - TV75Kapuas
5. Tunggu proses koneksi, akan muncul popup konfirmasi pada TV, yang menanyakan apakah Laptop yang akan terhubung tersebut diberikan akses atau tidak. Caranya klik Allow dengan menggunakan remote TV.
6. SmartTV siap digunakan.

## Metode HDMI

Pada tiap SmartTV yang ada di ruangan meeting, kami menyiapkan kabel HDMI direct untuk dihubungkan dengan perangkat yang memiliki HDMI output.

1. Colok kabel HDMI yang tersedia ke perangkat anda.

2. Pada TV akan muncul konfirmasi bahwa ada koneksi yang muncul, biasanya HDMI2.
3. Pilih HDMI2 pada dengan menggunakan Remote TV untuk menampilkan layar perangkat anda.

Kami merekomendasikan penggunaan kabel HDMI untuk koneksi layar, karena:

- Tampilan layar responsif, tidak delay
- Sangat jarang terkendala tampilan pecah-pecah atau terputus bahkan tidak bisa terkoneksi.

Kekurangan menggunakan Wireless Display:

- Tampilan layar sedikit delay.
- Pada laptop tertentu kadang ditemui kendala tampilan layar pecah-pecah, terputus berulang, atau bahkan tidak bisa terkoneksi.

Penanganan sederhana ketika ada masalah dengan SmartTV.

- Restart TV
  - Nyalakan TV
  - Tekan dan tahan tombol Power pada remote TV sampai TV hidup kembali.
  - TV sudah ter-restart
- Restart Laptop
  - Bisa dicoba untuk restart laptop setiap kali ingin memulai presentasi menggunakan TV
- Koneksi ulang pada WiFi
  - Lakukan Disconnect pada WiFi, kemudian Connect kembali ke nama WiFi sesuai ruangan meeting anda.
    - untuk Ruang Meeting Musi dan Brantas gunakan MBF-MGR
    - untuk Ruang Meeting Kapuas bisa menggunakan MBF-AP
    - untuk Ruang Meeting Mahakam di Plant bisa menggunakan MBF-AP-5G atau MBF-MAHAKAM

# WhatsApp anda kena retas?

## 1. **Uninstall dan Install Ulang WhatsApp:**

- Hapus aplikasi WhatsApp dari ponsel Anda.
- Unduh dan instal kembali aplikasi WhatsApp dari Google Play Store atau Apple App Store.
- Buka aplikasi dan masukkan nomor telepon Anda.
- Masukkan kode verifikasi 6 digit yang dikirim melalui SMS.

## 2. **Laporkan ke WhatsApp:**

- Jika Anda tidak bisa masuk karena verifikasi dua langkah telah diaktifkan oleh peretas, kirim email ke [support@whatsapp.com](mailto:support@whatsapp.com).
- Pada subjek email, tulis "My WhatsApp account got hacked" atau "Akun WhatsApp Saya telah dibajak".
- Jelaskan situasi Anda dan sertakan nomor telepon yang terkena hack dengan kode internasional (misalnya, +62 untuk Indonesia).
- WhatsApp akan menonaktifkan akun Anda sementara untuk mencegah penyalahgunaan lebih lanjut.

# PWA (Progressive Web App) dan panduan cara Instalasinya di iOS dan Android.

## Apa itu Aplikasi PWA?

PWA (Progressive Web App) adalah aplikasi web yang dirancang agar terasa dan berfungsi seperti aplikasi seluler asli. PWA dapat diakses melalui browser web, tetapi juga dapat diinstal ke layar utama perangkat Anda untuk akses cepat.

## Cara Menginstal PWA di iOS (iPhone/iPad)

Karena perubahan terbaru pada regulasi di Eropa, Apple telah melakukan beberapa perubahan pada dukungan PWA. Berikut langkah-langkah secara umum:

1. **Buka Safari:** Pastikan Anda menggunakan browser Safari di perangkat iOS Anda.
2. **Kunjungi Situs PWA:** Buka situs web PWA yang ingin Anda instal.
3. **Ketuk Ikon Bagikan:** Ikon ini biasanya terletak di bagian bawah layar Safari, berbentuk persegi dengan panah mengarah ke atas.
4. **Pilih "Tambah ke Layar Utama":** Gulir opsi di lembar bagikan hingga Anda menemukan "Tambah ke Layar Utama". Ketuk opsi tersebut.
5. **Konfirmasi dan Tambahkan:** Anda akan melihat pratinjau ikon dan nama PWA. Ketuk "Tambah" di sudut kanan atas.

## Cara Menginstal PWA di Android

1. **Buka Chrome (atau Browser Lain yang Mendukung):** Pastikan Anda menggunakan browser yang mendukung PWA, seperti Google Chrome.
2. **Kunjungi Situs PWA:** Buka situs web PWA yang ingin Anda instal.
3. **Cari Tombol "Instal":** Beberapa PWA akan menampilkan spanduk atau ikon "Instal" di bagian atas atau bawah layar. Anda juga mungkin melihat ikon "Instal" di bilah alamat browser.
4. **Ketuk "Instal":** Ketuk tombol "Instal" dan ikuti petunjuk di layar.
5. **Konfirmasi Pemasangan:** Konfirmasikan pemasangan PWA ke layar utama Anda.

## Hal yang Perlu Diperhatikan:

- **Keterbatasan iOS:** PWA di iOS mungkin memiliki beberapa keterbatasan dibandingkan aplikasi asli, seperti batasan pada proses latar belakang dan notifikasi push.
- **Manifest Aplikasi Web:** Agar situs web menjadi PWA, situs tersebut memerlukan manifest aplikasi web. Ini adalah file yang menyediakan informasi tentang bagaimana PWA harus ditampilkan dan berperilaku.
- **Perbedaan Browser:** Pengalaman PWA dapat sedikit berbeda tergantung pada browser yang Anda gunakan.

Semoga panduan ini bermanfaat!

# Modus Baru Bobol M-Banking Kuras Rekening Muncul di RI Jelang Lebaran

Ilustrasi penipuan mobile banking. (Dok. Freepik)

Masyarakat perlu berhati-hati dengan ancaman penipuan dengan modus phishing selama mudik lebaran nanti. Para penipu akan memanfaatkan momen liburan dengan peningkatan transaksi digital yang meningkat.

"Pada masa-masa liburan ketika transaksi digital meningkat dan kewaspadaan digital cenderung menurun, pelaku kejahatan siber kerap memanfaatkan rasa kepercayaan individu dan organisasi terhadap travel agency populer untuk mencuri data," kata National Technology Officer Microsoft Indonesia, Panji Wasmana, dalam keterangannya dikutip Senin (24/3/2025).

Microsoft Threat Intelligence mencatat serangan phishing tersebut menggunakan teknik Clickfix. Jadi data kredensial korban bakal bisa dicuri melalui laman login palsu serta captcha yang dibuat seperti aslinya.

Clickfix akan meminta korban melakukan perintah tertentu pada perangkat. Tanpa mereka sadari akan mengunduh malware pencuri data dan membuka akses ke HP pelaku.

Laporan tersebut menyebutkan Clickfix terus terjadi hingga Februari 2025. Serangan dilakukan di berbagai wilayah, termasuk menyerang Asia Tenggara.

Panji menjelaskan kita perlu mengenali pola serangan dan melakukan perlindungan. Dengan cara tersebut diharapkan dapat melindungi data dari para pelaku kejahatan.

"Dengan mengenali pola serangan dan mengambil langkah-langkah perlindungan, kita bisa mengurangi tingkat keberhasilan serangan, menjaga data, serta melindungi dunia digital kita. Mari, tetap waspada selama musim mudik," jelasnya.

Untuk menghindari menjadi korban phishing selama liburan lebaran nanti, berikut langkah-langkah perlindungan yang bisa Anda lakukan:

1. Pastikan berkomunikasi dengan hotel atau agen perjalanan resmi. Jangan lupa selalu mengecek kontak sesuai penyedia layanan tersebut.

2. Hanya gunakan jaringan yang aman dan hindari menggunakan Wifi publik saat login ke akun.
3. Selalu perikda alamat email yang diterima. Waspadai wmail phishing jika isinya mendesak melakukan sesuatu.
4. Jika mendapatkan email mencurigakan, hindari klik link yang tertera di dalamnya. Lakukan pengecekan lewat situs resmi.

**(dem/dem)**