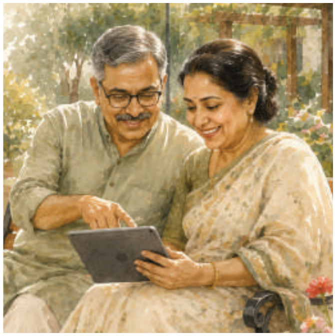
OPTIV

DSCI
PROMOTING DATA PROTECTION



A SIMPLE GUIDE TO STAY SAFE ONLINE


India
Meri Digital Suraksha
2026

ABOUT THE GUIDE

This safety guide has been created as part of Meri Digital Suraksha, a cyber security awareness initiative by DSCI in collaboration with Optiv.

It brings together essential areas like digital payments & online banking safety, email security, app security, social media safety, privacy protection, digital well being and cybercrime redressal into one practical handy guide that lays down best practices, cyber hygiene habits, and be aware of prevalent cyber scams and terminologies to remain vigilant and navigate the digital world more confidently.

WHAT'S INSIDE

CYBER SECURITY BEST PRACTICES

Everyday activities such as making digital payments, using apps, responding to emails and interacting on social media involve some level of cyber risk due to continuous cyberattack mechanisms from fraudsters.

Practising smart digital habits comes down to one golden rule: Pause, Verify and then Act on every call, message or link.

This section explains practical security habits across digital payments, app security, email and social media.

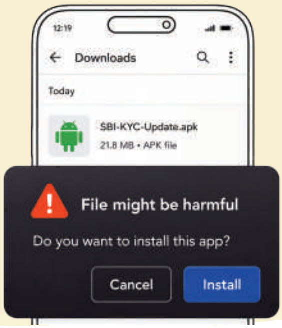
DIGITAL PAYMENTS & ONLINE BANKING SAFETY

Digital payments make everyday transactions quick and convenient, but they involve our money and financial information. **This is why digital payments and banking security matters: a fraudulent or incorrect transaction can put your money at risk and may become difficult to recover.**

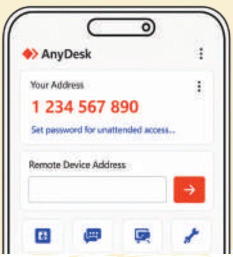
UNDERSTANDING COMMON DIGITAL TERMS

1 APK File

An APK (Android Package Kit) file is the standard format to install mobile apps in the Android operating system. Downloading and installing APK files from unknown websites, links, or messages carries major security risks, such as malware, data theft, and financial fraud.



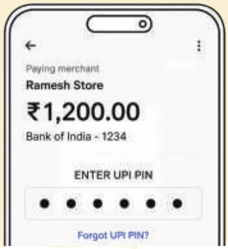
2 Remote Access/ Screen-Sharing App

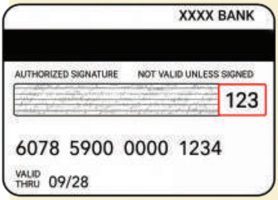


It is a software program that lets you show your device to another person and control your device from a different location, or to view your screen live. Common examples are **AnyDesk, TeamViewer, QuickSupport and RustDesk.**

3 UPI (Unified Payments Interface) PIN

A UPI PIN is a personal security code used to approve money transfers through UPI apps.



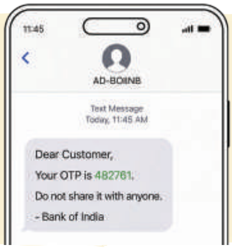


4 CVV

The CVV is a security code printed on your debit or credit card for online payments.

5 OTP (One-Time Password)

A temporary security code sent to your mobile number or email to verify a login or transaction.



6 KYC (Know Your Customer)

A process banks and apps use to check and verify a customer's real identity using official documents. Prevalent methods use eKYC, video KYC as well as the Central KYC (CKYC) to validate users.

7 QR Code

A QR code is a square barcode that can be scanned using your phone camera to complete digital actions such as payments.

BEST PRACTICES TO FOLLOW

- Use official banking and payment apps. Download them only from your phone's official app store; avoid links or APK files sent through messages.

- Never share your UPI PIN, OTP, credit/debit card CVV and PIN password or full card details with anyone.

- Verify the recipient and amount before approving any UPI payment, even if it says "refund," "cashback" or "prize."

- Always check the OTP SMS first to verify transaction amount and receiver's details before entering the OTP to make a payment.

- Be careful with QR codes. Scanning a QR code can make a payment; do not scan one simply to receive money or a refund.

- Don't give remote access to your phone. Never install a remote-access or screen-sharing app because an unknown caller asks you to.

- Ignore unexpected KYC calls or messages and contact your bank through its official channel.

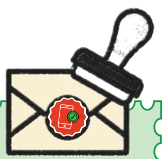
- Don’t let urgency influence a payment. Take time to independently verify requests involving fear, pressure or deadlines.

- Check your transaction alerts. Keep transaction notifications on and report anything unusual promptly.

- Set a UPI transaction limit. Set a daily limit that suits your needs to reduce your exposure if something goes wrong.

- Keep your bank account for your own transactions. Never let someone use it to receive or transfer money for a commission.

- Use official customer-care details. Get your bank’s number from its official website, app or passbook, not from messages or search results.



Always Remember

A UPI PIN is only needed to SEND money, never to RECEIVE it. If anyone asks for your PIN to give you a refund or cashback, it is always a scam.

COMMON DIGITAL PAYMENTS & BANKING SECURITY RELATED SCAMS

Fake KYC/Account Blocking Scam

A caller or message pretends to be from your bank and says your KYC needs to be updated or your account will be blocked. You may be directed to a fake website, asked to share details or told to make a payment.

Fake Refund/Cashback Scam

A message or caller claims that you are eligible for a refund, cashback or reward. You may be asked to approve a UPI request, scan a QR code or share payment details to receive it.

Remote Access Scam

A fraudster convinces you to install a remote-access or screen-sharing app, claiming it is needed to resolve a banking or payment issue. Once access is given, they may be able to view or control activity on your device.

Money Mule/Account Misuse Scam

Someone offers money or a commission for receiving and transferring money through your bank account. The money may have been obtained fraudulently, making your account part of the fraud.

QR Code Payment Scam

A fraudster sends or shows a QR code claiming it is needed to receive a payment, refund or reward. Scanning it can instead initiate a payment from your account.

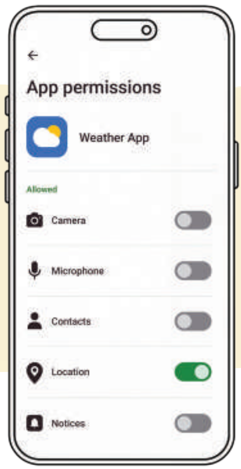
APP SECURITY

Apps make everyday tasks easier, but they can access different features and information on our phones. **This is why app security matters: an unsafe app can misuse this access, expose personal information or put your accounts and money at risk.**

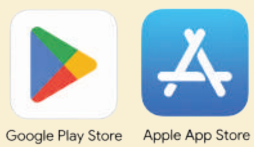
UNDERSTANDING COMMON DIGITAL TERMS

1 App Permissions

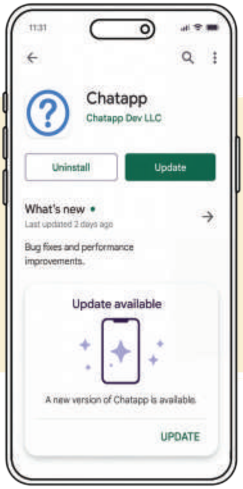
App permissions are the approvals you give an app to access certain features or information on your phone, such as your camera, microphone, contacts, photos or location.



2 Official App Store



The official app store is the trusted place provided by your phone manufacturer and operating system (OS) provider to download officially verified apps. On Android phones, this is usually the **Google Play Store**, and on iPhones, the **Apple App Store**.

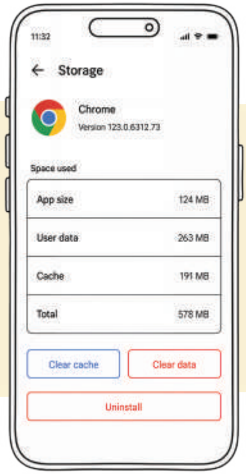


3 App Update

An app update is a newer version released by the app developer. It may fix problems, improve security or add new features.

4 App Cache/Data

App cache and data are information stored locally by an app on your phone. Cache usually consists of temporary files, while app data can include saved settings, preferences and other information.



BEST PRACTICES TO FOLLOW

- Use only the official app store and check the app name, developer, reviews and ratings before installing.

- Install only apps that you need. Avoid random apps suggested through social media, WhatsApp or messages, especially those offering trending features, rewards or games.

- Check app permissions. Give an app only the access it needs. A calculator does not need your contacts, and a simple photo-editing app does not need your location access.

- Keep your phone and apps updated. Install updates when available to fix security weaknesses.

- Create accounts only when necessary. Check what information the app asks for and whether you really need an account.

- Protect your phone and sensitive apps with a PIN, fingerprint or face lock, and enable two-factor authentication (2FA) for financial and other sensitive apps to prevent unauthorised access.

- Review your apps and permissions. Remove apps you no longer use and check that existing apps still have only the access they need.

- Pay attention to security warnings. If your phone or an app shows a security warning, stop and check before continuing.

- Verify an app before downloading and entering sensitive information. Never enter your OTP, PIN, password or banking details unless you are sure the app is genuine.

- Be careful with loan and investment apps. Verify the lender or investment company before downloading an app offering instant loans, guaranteed returns or quick profits.

Always Remember

Even apps on the official app store can sometimes be fraudulent or harmful. Before installing, check the app name, logo, developer and reviews to make sure you have found the genuine app.

FAKE APP SCAMS

A fake app is made to look like a genuine app so that you install it by mistake. It may use the same logo, colours and name as a trusted app, but small details may be different.

Fake Shopping App

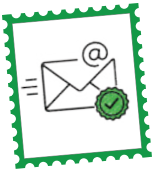
Fraudsters may create apps that offer heavily discounted products, limited-time deals or special offers. You may come across such promotions through Google searches, social media or messages. The app may look like a genuine shopping platform and take your payment without delivering the product.

Fake Government or Service App

Fraudsters may create apps that pretend to offer government services, subsidies, certificates, utility services or other public services. You may find such apps through Google searches, social media or messages. The app may look genuine and ask you to share Aadhaar, PAN, OTP or other personal information.

Fake Banking or Customer Support App

Fraudsters may create apps that pretend to be banking, payment or customer-support services. You may be directed to these apps through search results, messages or calls claiming to offer help with your account. The app may ask for sensitive information or permissions that can allow fraudsters to access your device or information.



EMAIL SECURITY

Email is part of our everyday digital life and often contains personal messages, documents and serves as a valid signup/login method.

This is why email security matters: if someone gets access to your email, they may misuse this information or use it to access your other accounts.

BEST PRACTICES TO FOLLOW

- To protect your email account, make a practice to always use a strong, unique password and turn on two factor authentication.

- Always check the sender’s email address before responding. Look for any inconsistencies or minor spelling errors to validate the address.

- Be careful with links. Don't click unknown links, especially those asking for payments, password resets, refunds or sensitive information.

- Be careful with attachments. Don't open unexpected PDFs, Word files, Excel sheets or other attachments, even from someone you know.

- Verify unexpected requests. If an email asks you to pay, share information or take urgent action, verify it through a separate, trusted channel.

- Avoid sending personal IDs, financial documents or other personal information via email. Only do so if it is utmost necessary and to trusted personally known email IDs.

- Keep your inbox organised. Remove sensitive documents and files you no longer need, and don't use email to store passwords, PINs or banking details.

- Manage spam and junk emails. If you don't recognise the sender or weren't expecting the email, mark it as spam or delete it.

- Don't share your device with others if it has your email logged in by default. Use app passwords for shared devices.

- Check for unfamiliar login and password-reset request emails autogenerated by service providers. This might indicate an invalid login attempt. Reset respective account passwords.

COMMON EMAIL PHISHING SCAMS

Phishing: It is the practice of tricking people into sharing personal or financial information, clicking harmful links, opening unsafe attachments or making payments by pretending to be a trusted person, company or organisation.

It is one of the most common ways cyber criminals use email to deceive people. A fake email may appear to come from your bank, courier company, government department or even a family member, and may create urgency to make you act without checking.

The following are some common forms of phishing and how they may appear in everyday situations.

Fake Bank/Account Update Email

A fake email claims your KYC, account, credit card or password needs updating and may threaten account blocking if not done.

Don't click such links or share any sensitive details. Check with your bank personally.

Fake Delivery/ Refund Email

A fake email claims your parcel is delayed, a refund is pending or a payment is needed.

Don't click the link or pay; check your order or refund through the company's official app or website.

Fake Family/Known Person Email

An email may appear to come from a family member, friend or someone you know and ask for money, information or urgent help.

Call them directly to confirm on such requests.

Fake Government Email

A fake email may claim to be from a government department and ask you to update personal details, pay a fine/challan or submit documents.

Don't click links or share documents; verify through the department's official website.

Fake Offers Email

A fake email may promise a prize, cashback, gift or discount and ask you to click a link, share details or pay a fee.

Don't act on unexpected offers; verify them through the company's official website or app.

Always Remember

A scammer may use different ways to contact you, but the trick is often the same; pretending to be someone you trust and getting you to click, share information or make a payment.

PHISHING
via Email

"Your bank account will be blocked. Update your KYC now."

"Your KYC has expired. Click here to update it."

SMISHING
via SMS/WhatsApp

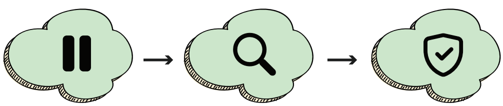
VISHING
via Phone Call

"I'm calling from your bank. Please verify your account details."

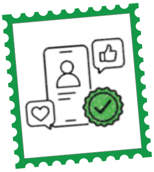
"Scan this QR code to receive your refund."

QUISHING
via QR Code

The channel may change, but the warning signs remain the same.



Pause → **Verify** → **Then Act**



SOCIAL MEDIA SAFETY

Social media helps us stay connected with family, colleagues, friends and community groups. We use it to share and receive photos, messages, videos and information from people we know and trust. But online content is not always genuine, and even familiar accounts can be fake or compromised. What we share can also expose personal information.

That's why social media safety matters: it helps us know what to trust, what to share, what to forward and who can see our information.

BEST PRACTICES TO FOLLOW

- Check your privacy settings regularly and choose who can see your profile, posts, photos and personal information.

- Think before you post and check whether a photo or post reveals your home address, location, phone number, travel plans, documents or other personal details.

- Check before believing or forwarding and verify surprising claims through a reliable or official source.
- Accept friend requests carefully and connect only with people you know or can verify.
- Verify unusual help or money requests from people you know by calling them directly on a number you already have.
- Be careful with links offering prizes, free gifts, unbelievable discounts or investment opportunities unless you have verified them.
- Keep sensitive information private and never share OTPs, PINs, passwords, banking details, IDs or important documents through social media.
- Be careful with direct messages from accounts pretending to be a friend's friend, distant relative or family friend. Always validate from respective friend/family member.
- Block and report suspicious accounts instead of continuing conversations that pressure, threaten or make you uncomfortable.
- Remember that social media sharing is not private, as private messages, photos and posts can be saved or forwarded.

HOW SOCIAL MEDIA-RELATED FRAUDS COMMONLY HAPPEN

Fake Family/Friend Account

A fake profile may use a family member's or friend's name and photograph to send a message asking for money or urgent help. If a request seems unusual or urgent, call the person directly on a number you already have before taking any action.

False or Misleading Information

A post, message or video may make claims about a government rule, health advice, financial opportunity or emergency and encourage people to forward it or pay a fee. Don't assume something is true because it has been widely shared; check it through a reliable or official source before believing or forwarding it.

Fake Prize/Giveaway/Offer

A post, page or message may claim that you have won a prize, received a special discount or been selected for a gift, and then ask you to click a link, provide financial information or pay a fee. Verify unexpected prizes or offers through the organisation's official website or app before responding.

Always Remember

Scammers can use details from your social media posts to make their messages sound personal and believable. Avoid sharing personal details publicly.

PRIVACY BEST PRACTICES

You may not realise it, but we share personal information every day when using apps, shopping online, making payments, booking travel, joining groups, filling forms or signing up for services. This can include our name, phone number, address, photographs, IDs, financial information and details about our family. Sharing information is often necessary, but sharing more than required can give others information they do not need.

Good privacy habits help you stay in control of what you share, with whom and why.

KNOW WHAT COUNTS AS PERSONAL INFORMATION

- Name, phone number and email
- Home address and date of birth
- Aadhaar, PAN, Passport, Voter ID & other identity documents
- Bank statements and financial information
- Photos and videos
- Location information
- Family's personal information (spouse, child, others)

PRIVACY BEST PRACTICES

- Share IDs and important documents only when necessary. Check who needs them, why they need them and use a trusted channel to share them.

- Check photos before posting or forwarding. Don’t share or mask documents, addresses, vehicle numbers, bills, locations or other personal information visible in the photo.

- Treat community groups as shareable spaces. Messages, photos and documents shared in family, RWA or other groups can still be saved, forwarded or used to spread fake news.

- Verify the recipient before sharing personal information. Check the name, phone number or email address before sending documents or other sensitive information.

- Avoid sharing personal information publicly. Don't post your phone number, home address, date of birth, family details or daily routine online.

- Respect others' privacy. Ask for permission before posting or forwarding someone else's photo, event or personal details digitally.

- Be careful about location and travel information. Avoid publicly sharing your live location, regular routine or plans that reveal when you are away from home.

- Delete personal information you no longer need. Remove old documents, screenshots, downloaded IDs and unnecessary files from your phone, chats and email.

- Check before clicking "Agree" or "Accept". Understand what information is being collected and for what purpose, and avoid providing extra information simply to access a service.

CHECK YOUR PRIVACY SETTINGS

Your privacy settings control who can see your information and what apps have access to your account. Check and review these settings regularly.

For Social Media

Keep your profile private where possible.	Don't include your full address, phone number, email or date of birth in your bio.	Limit who can see your posts, photos and stories.
Review who can follow or contact you and remove people you don't recognise.	Turn off location sharing unless you genuinely need it.	Review who can tag or mention you and approve tags where possible.

For Apps

Check access to your location, contacts, camera, microphone and photos.	Allow only the permissions an app genuinely needs.
Review apps connected to your Google, Apple, email or social-media accounts.	Delete account before removing apps you no longer use from your phone.

QUICK PRIVACY CHECKLIST

Before you share, post, download or agree, ask yourself.

- [ ] Am I sharing only what is necessary?
- [ ] Do I know who is asking for my details and why do they need it?
- [ ] Have I checked my privacy settings?
- [ ] Have I checked what an app can access?
- [ ] Have I checked the photo or document before sharing it?
- [ ] Would I be comfortable if this was saved or forwarded?

DIGITAL HYGIENE

Digital hygiene means following simple habits to keep your devices, accounts, passwords and online activities safe, organised and manageable.

Regular digital check-ups can help protect your information, reduce security risks and make technology easier to use.

DEVICE & ACCOUNT HYGIENE

We use our phones every day for communication, entertainment, payments, shopping and staying connected. Over time, we can end up with unused apps, old files, forgotten accounts and settings we no longer remember changing. **Intermittently checking your phone and online accounts helps keep your digital life organised, manageable and easier to use.**

REMEMBER TO

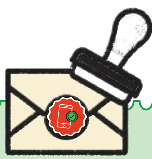
Is my phone clean & organised?

- **Check your apps:** Remove apps you no longer use and keep only those you need.
- **Check your storage:** Delete unnecessary photos, videos, downloads and files.
- **Check your notifications:** Turn off unwanted alerts, so your phone doesn't constantly demand your attention.
- **Check your accounts:** Review accounts you no longer use and close/delete them where appropriate.
- **Check your devices:** Sign out of accounts on phones, tablets or computers you no longer use.

Check your settings: Occasionally review important phone and account settings so you know what is switched on.

Check free trials and subscriptions: Check the price, renewal date and cancellation terms before starting a trial, and cancel subscriptions you no longer need.

Take a digital clean-up day: Every month, spend a few hours reviewing your phone, apps, accounts, settings and files.



A Simple Reminder

Just like you frequently organise your home, give your digital life a frequent clean-up too.

PASSWORD HYGIENE

We have multiple accounts for email, banking, shopping, social media, travel and other services. A weak or reused password can put more than one account at risk. **Good account security means using strong passwords and protecting your login details.**

What makes a strong password?

A strong password should be long, difficult to guess and different for each important account.

For example:

- ✗ charu123
- ✗ password123
- ✗ Using the same password for email, banking and social media

A better approach is to use a long passphrase made from unrelated words, with numbers or symbols where appropriate.

- ✓ Mango!River7Window

REMEMBER TO

- Use different passwords for important accounts. Keep separate passwords for your email, banking and other financial accounts.
- Turn on two-factor authentication. It adds an extra layer of protection beyond your password.
- Never share passwords, OTPs or verification codes with anyone.
- Change a password if you think it is compromised. Change it immediately if you have shared it accidentally or notice suspicious activity.
- Review old accounts. Close accounts you no longer use, especially those containing personal or financial information.
- Check where you are logged in. Sign out of devices or sessions you no longer recognise or use.
- Store passwords securely. Avoid writing them down near your phone or computer; use a reputable password manager if needed.

DIGITAL WELLBEING

Digital technology helps us stay connected with family, friends and communities. But spending too much time online, receiving constant notifications or feeling pressured to respond to every message can make digital life overwhelming. **Healthy digital habits help you stay connected without letting your phone take over your time, attention or peace of mind.**

Am I using technology in a healthy & comfortable way?

REMEMBER TO

- Don't feel pressured to respond immediately. Take your time, especially when a call, message or request feels urgent.
- Take regular breaks from your phone. Keep some phone-free time during meals, conversations, walks and before bedtime.
- Stay connected offline. Balance phone time with family, hobbies, walks and other activities.
- Protect your peace of mind. Mute, leave or ignore groups and conversations that become stressful or uncomfortable.
- Ask for help when unsure. If you don't understand an app, message, setting or notification, ask someone you trust before proceeding.

CYBERCRIME REDRESSAL

WHAT TO DO IF YOU FACE A CYBERCRIME?

Act immediately (but stay calm).
Do not wait or feel embarrassed about reporting the incident.

Inform your bank or payment service immediately.
Ask them to block or secure the affected account, card, UPI ID or transaction, as applicable.

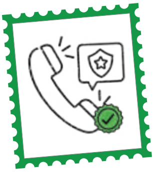
Preserve the evidence.
Save screenshots, transaction IDs, messages, phone numbers, email addresses, links and other details related to the incident.

Secure affected accounts.
Change passwords, enable two-step verification and block cards or payment services if required.

Report suspicious accounts or numbers.
Use the relevant platform or reporting service and block the account after saving the evidence.

If online reporting is not possible, visit your nearest police station or cybercrime police station.
Keep your complaint/reference details with you.

Keep track of your complaint.
Save the acknowledgement or complaint number and use it to follow up.



WHERE TO REPORT?

If you have faced a cybercrime or financial fraud

Call 1930 immediately to report a financial fraud. You can also register and track a cybercrime complaint online through the **National Cyber Crime Reporting Portal.**

Portal: cybercrime.gov.in

Helpline: 1930

If you receive a suspicious call, SMS or a message

Report suspected fraud communications through **Chakshu - Sanchar Saathi**. This includes suspected fraud calls, SMS and WhatsApp messages, including impersonation attempts.

www.sancharsaathi.gov.in

If you need support as a senior citizen

Call Elder Line - 14567 for guidance, support and assistance related to senior-citizen concerns.

If you need local police assistance

Visit your **nearest police station** or **cybercrime police station**. For emergencies or crimes other than cybercrime, contact the local police.

If your bank, card or UPI is involved

Contact your bank immediately using the **customer-care number** from your passbook, bank statement, official website or app.

Remember the Golden Hour

Lodge the complaint and contact your bank immediately within the first one hour of a financial fraud to maximise chances of financial recovery.

KEEP THIS INFORMATION READY WHEN REPORTING

- Date and time of the incident
- Amount lost, if any
- Transaction ID / UTR number
- Bank or UPI details involved
- Phone numbers and email addresses
- Screenshots of messages, profiles or websites
- Relevant links and account details
- Any complaint/reference number already received

OPTIV | DSCI
PROMOTING DATA PROTECTION

SHARING IS CARING FOR OTHERS' SAFETY.

Staying safe online starts with awareness. Share this guide with your family, friends and loved ones to help them navigate the digital world with confidence.

Want to keep the guide handy?
Scan the QR code to download your copy and revisit best practices whenever you need them.

DSCI_Connect dsci.connect dsci.connect dscivideo data-security-council-of-india

Data Security Council of India (DSCI), 4th Floor,
Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303.