MODULE 1:
CYBER SAFETY AWARENESS- MASTERCLASS

"Protecting Your Digital Life in the Real World"

Amit Dubey
Real World Defence
Not Just Theory

Course Duration	Total Segments	Requirements
3 Hours	7 Segments	Internet/Laptop

Learn how scams work, secure WhatsApp/Facebook, reduce tracking, and protect your money and identity. Practical cyber safety for everyday people — learn the settings and habits that block real-world fraud.

Module Objectives

A fast, practical masterclass for everyday users and working professionals. Learn how digital fraud actually happens, what platforms collect about you, and the simple security settings that reduce real-world risk immediately.

Most people don't need a degree to be safer online. They need: clarity on what's happening behind the screen, a few strong habits that prevent 80% of common attacks, and guided practice to set up accounts correctly. This masterclass is the first step in the Cyber-Sangh learning ecosystem: start with basics, then choose specialized modules based on your role (family, SME staff, creators, aspiring cyber roles

Who This Is For

This masterclass is designed for:
•Individuals who want to protect their accounts, money, and identity
•Students and first-jobbers building safe digital habits early
•Parents and families managing devices, UPI, social media, and privacy
•SME owners and teams handling customer

Teaching Format

•Live demonstrations (safe, awareness-only)
•Guided verification exercises (participants follow along)
•Real case breakdowns + clear "what to do next" rules

Certificate: Certificate of Completion (non-degree)
Designed by: Cybercrime Expert Amit Dubey

FAQs

Is this a degree or certification?

No. This is a short, practical masterclass with a Certificate of Completion.

Do I need technical knowledge or coding?

No. This masterclass is designed for normal users and working professionals. No coding or technical background is required.

Will we do real exercises?

Yes. Participants will audit their own settings live (guided), and we will run real tracking demonstrations during the session.

Is this suitable for SMEs?

Yes. We also offer a group version tailored for SME teams, focusing on staff roles and common business risk patterns.

Will you teach hacking?

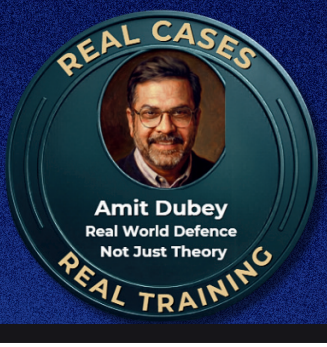
No. The focus is awareness, prevention, and safe configuration. Any attack patterns shown are only for helping participants recognize and stop fraud.

What You Get

- Guided Account Audit Checklist
- Safety Rules You Can Apply Immediately
- Digital Life Protection" Personal Action Plan
- Certificate of Completion

Skills you gain

- Ability to trace digital clues
- Identify fak identities
- Detect deepfakes & impersonation
- Understand how investigators think
- Protect themselves & guide others



Curriculum

SEGMENT 1.1: Data Safety — Facebook & Google (Your Digital Shadow)

What You Learn
This section explores what data Facebook and Google collect, the difference between data you share vs data they infer, and how advertisers, scammers, and attackers use this data.
Live Demo
This section explores the Google "My Activity" dashboard, location history and device activity, and Facebook Ad Preferences: interests + behavioral tags.
Hands-on Exercise
Participants audit their accounts live and disable multiple high-risk tracking features.

SEGMENT1. 2: Privacy Analyzer — Who Is Tracking You?

Key Concepts
This section explores trackers vs cookies vs fingerprinting, how websites profile users silently, and data leakage through browsers and apps.
Live Demo
This section explores running a privacy analyzer on common categories such as news sites, e-commerce sites, and public service portals, and shows real-time trackers firing.
Outcome
Participants see tracking in real time and learn safer browsing habits immediately.

SEGMENT 1.3: Securing WhatsApp (Most Abused Platform)

Threats Covered
This section explores account takeover basics, "WhatsApp cloning" myths vs reality, and fake support and verification scams.
Live Demonstration
This section explores enabling 2-step verification, checking linked devices, and recognizing fake "WhatsApp Team" messages.

SEGMENT 1.4: Securing Facebook (Account Hijack Prevention)

Attack Vectors
This section explores phishing login pages, fake copyright notices, and friend impersonation scams.
Practical Steps
This section explores securing email first (root access principle), enabling login alerts, removing suspicious sessions, and locking recovery options.
Audience Exercise
Participants spot the difference between a fake Facebook email and a real one.

SEGMENT 1.5: OTP Theft Techniques (How Scammers Steal It)

Real-World Techniques Explained
This section explores social engineering calls, fake KYC update links, screen-sharing app misuse, and SIM swap basics (awareness-focused).

Live Role-Play
Participants experience the manipulation flow so they can recognize it in real life.

Core Lesson to Remember
Key takeaways reinforce recognizing manipulation patterns and responding safely in real situations.

SEGMENT1.6: Mobile Hardening Framework (MobiArmour Approach)

A practical mobile security framework (not "one app that solves it all").

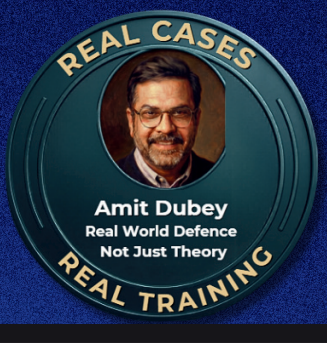
Protection Layers
This section explores protection layers, app permission hygiene, rogue / over-permissioned app detection, device lock + backup discipline, and public Wi-Fi safety.

Live Demo
Identify risky permissions and remove spyware-like apps.

Module 7: Case Studies — Real Incidents, Real Learnings

A rapid, high-impact walkthrough of modern fraud patterns, including:

1.Digital arrest fraud
2.Trading/crypto investment fraud
3.Loan app scams
4.AI voice cloning fraud
5.APK fraud via wedding/birthday "cards"
6.Electricity bill / courier scams
7.UPI "collect request" and payment link fraud
8.OTP & Screen-sharing scams (AnyDesk/TeamViewer patterns)
9.Fake investment & lottery schemes
10.Romance scams, Social Media impersonation, deepfakes
11.Fake customer support and helpline numbers, Fake App downloads
12.Phishing across email/SMS/WhatsApp
13.Identity theft and SIM swap indicators
14.Booking fraud /online shopping and discount fraud(travel/temple/hotel packages)
15.Sextortion response basics (evidence, reporting, do-not-pay rule)



SEGMENT 7: Case Studies — Details

CASE STUDY 1: DIGITAL ARREST FRAUD

Attack Narrative

- Victim receives call claiming to be from Police / CBI / Customs
- Accused of money laundering / parcel with drugs
- Threat of "digital arrest on video call"

Key Manipulation

- Fear + authority + urgency

Learning Outcome

Police never arrest on video call

Courts do not operate on WhatsApp or Zoom

CASE STUDY 2: SHARE TRADING / CRYPTO INVESTMENT FRAUD

Attack Narrative

- Telegram / WhatsApp group showing fake profits
- Initial small gains allowed
- Bigger investment → withdrawal blocked

Technical Trick

- Fake trading dashboards
- Screenshots & cloned apps

Golden Rule

"If returns are guaranteed, fraud is guaranteed."

CASE STUDY 3: LOAN APPS FRAUD

Attack Narrative

- Easy loan → excessive permissions
- Contacts, photos exfiltrated
- Harassment & blackmail for repayment

Technical Insight

- Permission abuse
- Offshore servers

CASE STUDY 4: AI VOICE CLONING FRAUD

Attack Narrative:

Call in voice of:

- Son / daughter
- Boss / CEO

Emergency money demand

Reality:

- 10–30 seconds of voice sample is enough for cloning

Defense:

- Call back verification
- Family password protocol

CASE STUDY 5: APK FRAUD – WEDDING / BIRTHDAY CARD

Attack Narrative
APK sent as:
- Wedding invitation
- Birthday card

User installs → phone compromised
Malware Capability
- OTP reading
- Screen overlay
- Banking access

CASE STUDY 6: ELECTRICITY BILL / COURIER FRAUD

Attack Narrative
- "Bill pending, power will be cut"
- "Courier with illegal item seized"

Key Learning
- Utilities do not demand instant payment via links.
- Courier companies don't conduct criminal inquiries

CASE STUDY 7: UPI & BANKING PAYMENT LINK FRAUD

Attack Narrative
- "Collect money" disguised as "Pay money"
- QR code misuse
- Fake refund screens

Rule
- "You never need to pay to receive money."

CASE STUDY 8: OTP & SCREEN-SHARING SCAMS

Tools Misused
- AnyDesk
- TeamViewer
- Quick Support
- Zoom / Google Meet

Attack Flow
- Screen share → OTP visible → account takeover

Hard Rule
- Banks never ask to install apps

CASE STUDY 9: FAKE INVESTMENT & LOTTERY SCHEMES

Attack Narrative
- "You've won a prize"
- Processing / tax fee demanded

Reality
Legitimate lotteries never charge winners

CASE STUDY 10: SOCIAL MEDIA IMPERSONATION & ROMANCE SCAMS

Attack Narrative
- Fake profiles
- Emotional bonding
- Gradual financial dependency

Psychology Used
- Loneliness
- Trust-building over weeks

CASE STUDY 11: DEEPFAKE VIDEO & VOICE CALLS

Threat Evolution
- Video calls with synthetic faces
- Fake executives giving instructions

Defense
Secondary verification channels
Delay decisions under pressure

CASE STUDY 12: TECH SUPPORT & FAKE APP DOWNLOADS

Attack Narrative
- Fake pop-ups:
- "Virus detected"
- Fake Play Store / App Store links

Damage
- Remote access
- Data theft

CASE STUDY 13: IDENTITY THEFT & SIM SWAP

Attack Narrative

- SIM suddenly stops working
- Bank accounts drained

Indicators

- Network loss
- Password reset alerts

CASE STUDY 14: ONLINE SHOPPING & DISCOUNT APP FRAUD

Examples

- Fake Amazon / Flipkart links
- Unreal discounts

Clue

Fake domains
No COD option

CASE STUDY 15: HOTEL / TEMPLE / KEDARNATH / CRUISE BOOKINGS

Attack Narrative

- Fake Instagram pages
- Advance payment
- No booking confirmation

Learning

Always cross-verify on official websites

CASE STUDY 16: FAKE CUSTOMER SUPPORT / HELPLINE NUMBERS

Attack Narrative

- Google search → fake helpline
- Victim calls scammer directly

Rule

Never trust helpline numbers from ads

CASE STUDY 17: PHISHING (EMAIL, SMS, WHATSAPP)

Attack Vectors

- Fake KYC
- Account suspension alerts

Key Insight

URLs reveal truth, not logos

CASE STUDY 18: SEXTORTION – Online Blackmail, Digital Exploitation & Cyber Threats

This section explores an **attack** narrative involving fake video calls, recording threats, and blackmail. It outlines the response strategy: do not pay, preserve evidence, and report immediately.

Core Takeaway:
"Fraud does not begin with technology. It begins with emotion manipulation."