

CYBER BULLETIN

HACK GEAR 2024

1. WIFI PINEAPPLE

HAK5



TARGET: Wi-Fi networks and connected devices that lack strong security measures.

IMPACT: Potential for unauthorized data access, interception of communications, and network compromise.

MITIGATION: Employ robust encryption (WPA3), keep devices and firmware up-to-date, and implement network monitoring and intrusion detection systems.

3. FLIPPER ZERO

ALEX AND PAVEL



TARGET: Radio frequency (RF) devices, RFID/NFC systems, and infrared (IR) communication.

IMPACT: Risk of unauthorized access, data interception, and device manipulation.

MITIGATION: Secure RFID/NFC with encryption, regularly update device firmware, and limit physical access to sensitive devices.

5. DSTIKE WATCH V3

MOKXIHIT



TARGET: Wi-Fi networks and devices, including IoT devices.

IMPACT: Risk of unauthorized network access, data interception, and device control.

MITIGATION: Use strong Wi-Fi encryption (WPA3), keep firmware up-to-date, and employ network monitoring tools to detect and respond to suspicious activity.

2. HACKRF ONE

GREAT SCOTT GADGETS



TARGET: Wireless communication systems across various frequencies.

IMPACT: Potential for eavesdropping, signal interception, and unauthorized control of wireless devices.

MITIGATION: Use strong encryption for communication, regularly update firmware, and secure wireless systems against unauthorized access.

4. UBERTOOTH ONE

MICHAEL OSSMANN



TARGET: Bluetooth devices and communication channels.

IMPACT: Unauthorized data access, and Bluetooth communication interception.

MITIGATION: Use strong pairing protocols, keep Bluetooth devices updated, and disable Bluetooth when not in use.

6. OMG CABLE

MIKE GROVER



TARGET: Devices and networks using Ethernet or USB interfaces.

IMPACT: Potential for unauthorized data access, device manipulation, or network compromise.

MITIGATION: Use physical security measures, secure device configurations, and monitor for unusual network activity.



संयुक्त सूचना एवं
सूचना प्रौद्योगिकी विभाग
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY



STAY SAFE ONLINE
अनिलान सुरक्षा कवाच



Digital India
Power To Empower

**Quad Cyber
Challenge**

5 STEPS YOU CAN TAKE TO PROTECT YOUR DIGITAL FOOTPRINT



**# Be Safe
Stay Safe**
www.staysafeonline.in

- Practice good digital hygiene
- Adjust your browser settings
- Maintain separate accounts
- Make your digital profile informal
- Do not enter your personal information in third-party websites

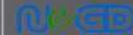
In association with

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE



साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre



my GOV
मेरी सरकार



www.
InfoSec
awareness.in

CYBER SAKCHARTA ABHIYAN
UNDER THE AEGIS OF
CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION

FACULTY COORDINATORS

Mr. SHUBHAM KUMAR | Mr. FAIZAN MAHMOOD

STUDENTS COORDINATORS

MOHAMMAD FARHAN | SIDRA SIDDIQUI | ELMA SHARIQ | ADEEBA KHATOON

Prof. (Dr.) MOHAMMAD FAISAL
Head, Department of Computer Application