Report findings will support coordinated action in Africa against cybercrime.

A new report published by INTERPOL gives key insights into cybercrime in Africa. The result of cross-sector collaboration, the African Cyberthreat Assessment Report 2021 will help countries in Africa to understand the most prevalent threats and formulate a coordinated regional response to cybercrime.

Digital transformation

Cybercrimes affect all countries, but weak networks and security make countries in Africa particularly vulnerable.

While Africa has an estimated 500 million Internet users, this equates to just 38 per cent of the population, leaving huge potential for growth. Africa has the fastest growing telephone and Internet networks in the world, and makes the widest use of mobile banking services.

This digital demand, coupled with a lack of cybersecurity policies and standards, exposes online services to major risks. As African countries move to incorporate digital infrastructure into all aspects of society – including government, banking, business and critical infrastructure – it is crucial to put a robust cybersecurity framework into place.

The main cyberthreats in Africa

The INTERPOL report identifies the most prominent threats in Africa, based on input from INTERPOL member countries and data drawn from private sector partners.

The top five threats are:

* **Online scams**: fake emails or text messages claiming to be from a legitimate source are used to trick individuals into revealing personal or financial information;
* **Digital extortion**: victims are tricked into sharing sexually compromising images which are used for blackmail;
* **Business email compromise**: criminals hack into email systems to gain information about corporate payment systems, then deceive company employees into transferring money into their bank account;
* **Ransomware**: cybercriminals block the computer systems of hospitals and public institutions, then demand money to restore functionality;
* **Botnets**: networks of compromised machines are used as a tool to automate large-scale cyberattacks.

From analysis to action

“Not only do criminals exploit vulnerabilities in cyber security across the region, but they also take advantage of variations in law enforcement capabilities across physical borders,” said Craig Jones, INTERPOL’s Director of Cybercrime.

“INTERPOL’s regional cybercrime strategy for Africa provides a robust framework for sharing intelligence and coordinating action to strengthen the law enforcement response across Africa and beyond,” added Mr Jones.

The strategy focuses on the areas of criminal intelligence, law enforcement operations, regional capacity and capabilities, and awareness campaigns for businesses and the general public.

Implementation will be driven by INTERPOL’s African Cybercrime Operations Desk, working in close partnership with key regional stakeholders, in particular the African Union and Afripol, law enforcement communities and the private sector

**DIFFERENT TYPES OF CYBERCRIME**

Malware is software that cybercriminals use to disrupt their target’s network. This software is often downloaded by the target without their consent via different forms of contact such as emails, clicking on malicious links, and drive-by downloads.

The following are some examples of cybercrime, some of which utilize malware to gain access to the desired information:

* **DDoS Attacks:** These attacks are effective by making online service unavailable/taking entire networks down. Hackers do this by overwhelming the target’s network or site with traffic from multiple sources. Hackers then create and deposit malware known as Botnets onto users’ computers, allowing them to hack into their system while the network is down.
* **Botnets:** As we went over just a moment ago, Botnets are not your friend. They are networks that reside in a compromised computer system, allowing control of the system by an external user - usually a cybercriminal. These remote hackers then send the user spam or sometimes even attack other computers through the botnets. Botnets are also able to function as malware, causing significant harm to a user’s system as it carries out malicious tasks.
* **Identity Fraud:** According to the [FBI Internet Crime Report of 2021](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf), more than 300,000 Americans fall for identity theft through many different forms of cybercrime. Identity fraud or identity theft occurs when a cybercriminal gains access to a victim’s personal information. This can include name, birthday, social security number, and passport number. Information like this allows criminals to gain access to someone’s funds and confidential information, among many other serious offenses.
* **Social Engineering:** This tactic by cybercriminals involves gaining a victim’s trust by direct communication through either phone or email. Oftentimes, they will pose as customer service representatives in hopes of gaining passwords to hack into your account. From there, the cybercriminal can gain access to your bank account or simply sell your information.
* **Ransomware:** If the name of this cybercrime tactic sounds scary to you, it’s because it is. Much like asking for a ransom in a kidnapping situation, cybercriminals will hack your system and take your information, only to turn around and demand a ransom for you to get it back. Usually, they ask for large amounts of money.
* **Phishing:** [Phishing](https://etactics.com/blog/how-to-spot-phishing-email) is one of the most prevalent forms of cybercrime today, with an [estimated 3.4 billion spam emails](https://aag-it.com/the-latest-phishing-statistics/#:~:text=Phishing%20is%20the%20most%20common,common%20cause%20of%20data%20breaches.) sent out a day. Phishing involves hackers sending emails that contain malicious attachments or URLs. If victims click on these links, their system opens to the hacker and allows them to gain access to your sensitive information.

Real-Life Cybercrime Examples

**MGM: SEPTEMBER 2023**

MGM Resorts reported on September 11, 2023 that a “cybersecurity issue” began affecting some of its systems. The hotel/casino chain promptly shut down these systems in order to protect themselves. Subsequently, hotel room digital keys and slot machines were out of order, causing nothing short of chaos for resort guests and the organization itself.

Reports that the hackers used an employee's information on LinkedIn to impersonate them in a call to MGM’s IT help desk. This act of social engineering allowed the cybercriminals to then gain access to that employee’s credentials. Though, MGM has not confirmed this.

While rumors continued to spread, MGM did not respond to a request for information on who was behind the attack.

**OREGON AND LOUISIANA DEPARTMENTS OF MOTOR VEHICLES: JUNE 2023**

One of the organizations directly affected by the MOVEit software breach happens to be our next example. The US states of Oregon and Louisiana reported that their departments of motor vehicles experienced data loss. Louisiana’s Office of Motor Vehicles (OMV) reported at least 6 million records stolen. Meanwhile, the Oregon Department of Motor Vehicles (DMV) estimated around 3.5 million stolen driver’s licenses and identity cards.

The states’ third-party software breach resulted in leaked personal information such as names, addresses and birthdates, Social Security numbers, vehicle registration numbers and handicap information.

**MOVEIT: MAY 2023**

The largest hack of 2023, not to mention one of the largest in recent history, belongs to MOVEit. Everything began in May of 2023 when [Progress](https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023) discovered a vulnerability in MOVEit Transfer. For reference, MOVEit Transfer is their file transfer service which thousands of organizations utilize around the world. Data moved through this service is often sensitive in nature.

This vulnerability allowed hackers to infiltrate the servers and steal these organization’s sensitive information within. Most notably a notorious ransomware and extortion cybergang by the name of Clop is taking advantage of this security vulnerability.

So far the number of organizations [affected by this breach is over](https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJ65BhbFxLhlNeEIQC0i725_tuomxUhupWH-3qlm78_CZD72dqPq3Ub4uF5wQaCMdbLjv2Ug8BXz9ZMfYfgN0DZKOMp03yZQJ0SLLDjNIT4AIjA9KtdjFDuff-80tc59ZW2aTG2yvMLO1WegR74MWmMJLYNcJNcxlsvCipXVRyqe) 1,000, and the number of individuals affected is sitting around 60 million. Experts expect numbers to rise as time goes on and more organizations confirm their MOVEit security breaches.

**SHIELDS HEALTH CARE GROUP: APRIL 2023**

April 2023’s largest data breach was due to a cybercriminal gaining unauthorized access to the Shields Health Care Group’s systems. This Massachusetts-based medical services provider reported the personal data leak of over 2.3 million people.

The incident, according to Shields, dates back to March 2022, when they first noticed suspicious activity on their servers. The organization followed protocol by sending letters to individuals affected. However, the firm’s investigation concluded this year and was able to fully reveal the scale of the damage. Sensitive data extracted by cybercriminals in the two weeks the breach was active included:

* Patients’ Social Security numbers.
* Dates of birth, home addresses.
* Healthcare provider information.
* Healthcare history.
* Billing information.
* Insurance numbers.

**LATITUDE FINANCIAL: MARCH 2023**

In March of 2023, the Melbourne-based company Latitude Financial suffered a security breach resulting in the compromise of more than 14 million records. The company, which provides loans and credit cards, reports that the cybercriminals captured several different types of data in their attack.

Nearly 8 million driver’s licenses, along with 53,000 passport numbers fell into the hands of these hackers. The list of compromised data continues as dozens of monthly financial statements and an additional 6 million records dating back to 2005 became compromised at this time.

Unfortunately, public scrutiny over this breach intensified as originally Latitude Financial reported the attack only affected 300,000 people.

How to Avoid Cyberattacks

So how can you avoid falling into a cyber scam? Here are a few steps that individuals and organizations can take to protect personal information and avoid financial damage.

* Update your software and operating system regularly. This ensures you are benefiting from the latest security patches to protect your computer and network system.
* Invest in anti-virus protection. Using a comprehensive internet security solution allows you to scan your computer, which helps detect any threats before they become a problem.
* Use strong passwords and be sure to NOT record them anywhere.
* Do not open attachments in emails from senders you don’t know.
* Do not click on links sent from unknown sources.
* Do not give out personal information unless it is through a secure network.