Rhombixtechnologies_tasks3

Topic: RFID Blocking

Name: Qamash Bashir

Domain: Cybersecurity

Month3

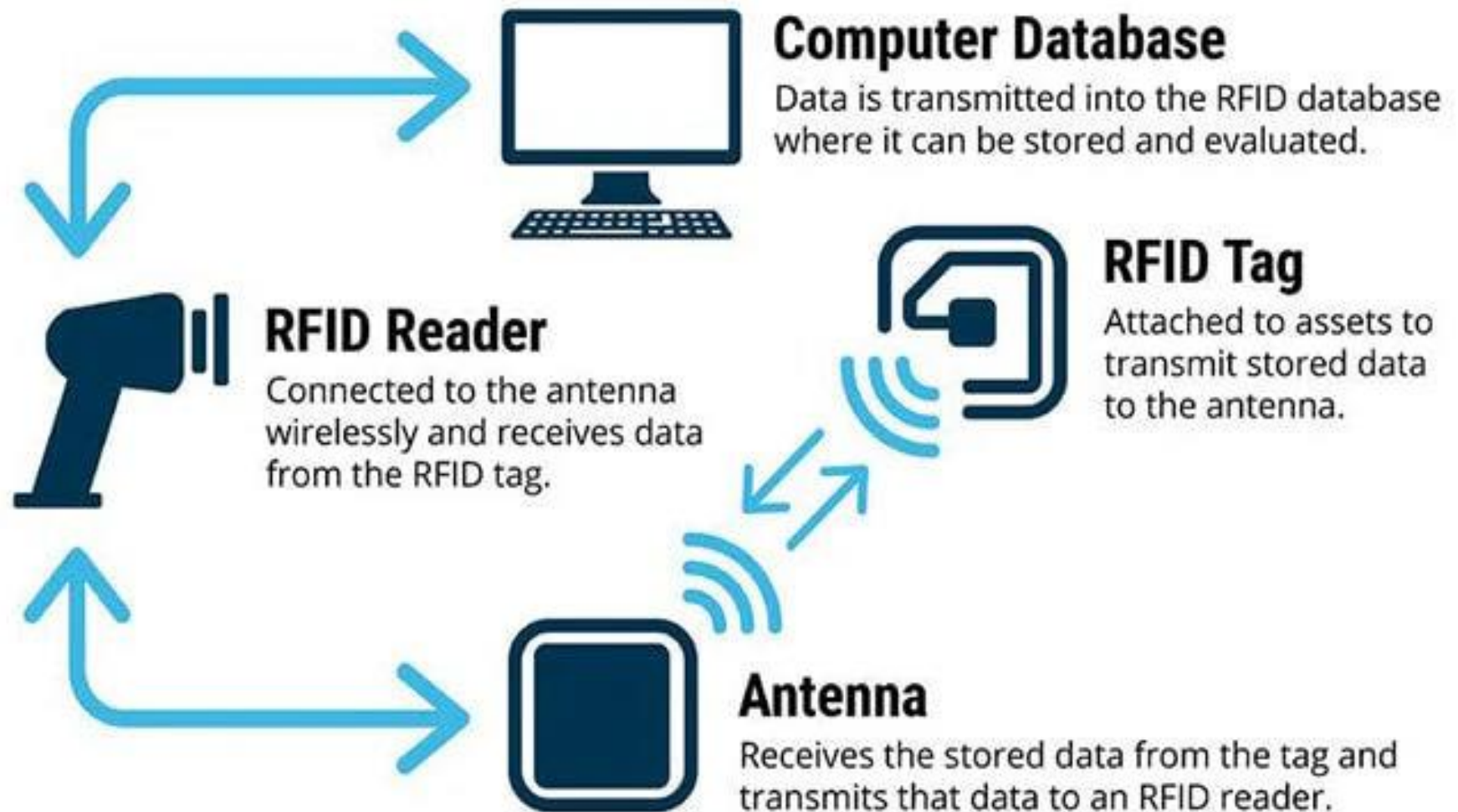# RFID blocking

- **What is RFID?**

The full meaning of RFID is "Radio Frequency Identification" a technology that allows machines to read signals from RFID chips implanted in passports and credit cards to transact over a short distance. RFID technology is a critical component of modern contactless payments, but it has raised concerns about possible vulnerabilities to criminal manipulation.

What is RFID blocking?

RFID blocking is the process of making your RFID-enabled device resistant to unauthorized access. The most popular way to achieve this is by getting an RFID blocking wallet — a holder for your cards that is made from materials that interfere with electromagnetic fields.

- RFID blocking technology was developed to prevent criminals from taking advantage of no-authorization contactless scanning. In theory, a thief standing nearby could surreptitiously access your card's RFID function in what is known as a "skimming" attack, leeching money from victims in the street, a crowded bus, or a queue at the grocery store.

Computer Database
Data is transmitted into the RFID database where it can be stored and evaluated.

RFID Tag
Attached to assets to transmit stored data to the antenna.

RFID Reader
Connected to the antenna wirelessly and receives data from the RFID tag.

Antenna
Receives the stored data from the tag and transmits that data to an RFID reader.

RFID tags

Physical structure: RFID tags comprise an integrated circuit (IC) or microchip and an antenna. The IC contains non-volatile memory, which stores data and a unique identification number.

Frequency bands: RFID tags operate in different frequency bands, such as low frequency (LF: 125 kHz and 134 kHz), high frequency (HF: 13.56 MHz), and ultra-high frequency (UHF: 860-960 MHz). Each frequency band has its advantages in terms of read range, data transfer speed, and resistance to interference.

Data transfer: When energized by an RFID reader's radio waves, the tag's antenna receives power and activates the IC. The IC then modulates the radio waves and backscatters them to the reader, transmitting the stored data (UID and additional information).

Types of tags: RFID tags can be categorized as passive, active, or semi-passive (battery-assisted passive). Passive tags rely on the reader's energy for power, while active tags have their own power source (battery) to actively transmit signals. Semi-passive tags use the reader's energy for powering the IC but have a battery for signal transmission.

Does RFID blocking really work?

- RFID blocking materials can effectively prevent the scanning function on a card or passport, and the range of products that boast this feature is steadily growing.

- Everything from wallets to waterproof fanny packs now support RFID blocking capabilities. A layer of carbon fiber or aluminum can protect you from contactless attacks, and that's a key selling point for some items.

Do I need RFID blocking?

You might have seen reports claiming that "contactless crime" can result in huge financial losses. The problem is the studies used to support these claims don't make a compelling case for RFID blocking specifically.

If a victim loses money in a "contactless-related" event, it's almost always because their card was physically stolen from them. For example, in a 2018 report, UK Finance found no record of any contactless theft occurring that year while a card was still in the possession of its owner. Even in this scenario, the damage would be capped to the contactless payment threshold.

There are four key reasons why outright contactless attacks are unlikely:

- When scanned, credit cards use a one-time transaction code to complete the process, and that code is heavily encrypted.

- The scanable information on a card doesn't include the sensitive data that thieves are actually looking for (the CVV code on the back of the card, for example).

- To steal their data, an identity thief would have to get physically close to the victim. The risk of being caught in the act and captured on CCTV, with no guarantee that the target's card will even be accessible, is a strong deterrent.
- Criminals no longer need to risk getting close to victims or use credit card skimmers because huge lists of compromised credit card details are readily available on the dark web.

Does RFID blocking prevent identity theft?

RFID blocking tools claim to [protect users against identity theft](#) by stopping criminals from scanning your passport's ID chip by just rubbing shoulders with you. In practice, however, RFID blocking does little to help in the most likely identity theft scenarios.

The information available via RFID is completely encrypted — manufacturers know how sensitive it is. In the majority of cases, the data is accessible only to the kind of verified scanners you'll encounter at airports and other official checkpoints. Furthermore, most passports issued in the last decade already contain layers of RFID blocking material.

Anxiety around identity theft is understandable. In a nightmare scenario, this crime could haunt victims for years after their personal details have been stolen. In some cases, the damage is impossible to undo. But adding further physical protection won't do much for security — the real threats are online.

Genuine security begins with encryption

Today's criminals know that if they want to extract money and sensitive data from their victims, they don't need to do it in person. From the social engineering of a phishing email to the insidious probing of an extortion kit, there are plenty of reasons to be concerned.

You need a different kind of protection, one that actually responds to the challenges you face. NordVPN provides powerful encryption, strengthening security and enhancing personal privacy.

NordVPN's [Dark Web Monitor](#) feature will also alert you if your account credentials have been found on underground hacker hangouts, letting you protect yourself before they act.

So don't wrap your credit card in tinfoil — choose real security for online activities.

The END