What about privacy and privacy issues if VR and AR are hacked?

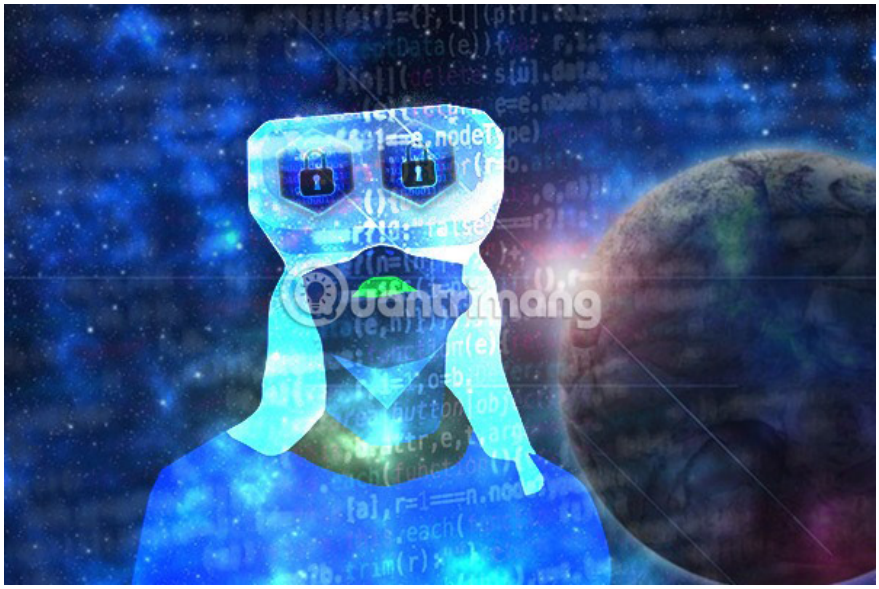
VR and AR may be an inevitable part of life in the future, which means they will almost certainly become the target for those who want to use these devices to exploit the benefits of people. use.

Virtual reality (VR) and augmented reality (AR) technology can become an inevitable part of life in the future, meaning they are almost certainly the target for those who want to use it. These devices to exploit the benefits from users. To some extent, these devices don't really bring too much risk. Users have entered credit card information and brought with them Internet-connected cameras for a long time and VR or AR technology is really just a new kind of 'interface' to perform the same task. . However, depending on how technology evolves, there may be certain risks to security and privacy, even to the real world.

How does VR and AR hack affect security and privacy?

1. Security risks from VR / AR
2. Digital copies
3. Digital money
4. Attack the Human joystick
5. When the virtual world directly affects the physical world
6. Privacy risks
7. Eye movement
8. Body movement and other data
9. Physical environment
10. Virtual environment
11. Never use a VR headset is it safer?

Security risks from VR / AR



Fortunately, sophisticated tracking data is created in the virtual world - with a lot of head, hand, body and eye movement - not attractive to criminals. They often like details about bank card types and how users send these information over the Internet at all times. However, vulnerable VR systems give rise to a number of new security risks.

Digital copies

When both VR and criminals become more sophisticated, they can access your voice, behavior and movement data, create your digital copy and use it to impersonate you with bad purpose. If using VR for work, social interaction or shopping, having a fake "twin version" just keeps going badly and it can even be used as a ransomware.

Digital money

A more obvious problem is what can happen if someone has sensitive content that is spread out. People often have great demand for 'adult' VR entertainment and VR offers a wide variety of options, so there may be some things that are recorded without the user's knowledge. Some of these records will almost certainly be an attractive blackmail document for cyber criminals.

Attack the Human joystick

VR hacking can also penetrate the physical world. Researchers have developed and tested software that allows them to edit the virtual environment in a way that users are manipulated to move physics in a certain direction, called a Human joystick attack. Because now you seem to be in a state of "blindness" with a VR headset, this may result in you falling down the stairs or in danger.

When the virtual world directly affects the physical world

If people rely on virtual reality technology or augmented reality to relay important information in everyday life, these systems need to be very secure. For example, doctors have the ability to use AR to support viewing medical data and performing procedures. If hackers can change the feed, they will likely harm the patient.

Even everyday tasks, such as shopping in virtual supermarkets or reading AR information on highway signs, can also be altered in a way that could threaten human life. A DDoS attack aimed at these systems can cause them to crash and create crisis for AR-dependent people and places.

Privacy risks

Security risks are still not a big problem, because there simply aren't enough AR / VR devices used to create extremely dangerous threats. Even so, privacy is a problem that many people are concerned about, sophisticated tracking data and environmental data created in the VR / AR world that are going to places where users may disagree. .

Eye movement

Websites and advertisers always want to find user behavior, knowing exactly what users are watching, and how long it is worth much more than the current user numbers. User behavioral monitoring data has been used to target ads and provide analytics, as well as being able to be used to conduct secret tests and create psychological profiles about people. use.

Body movement and other data

User's eye movement may be the most valuable, but tracking the rest of the body is also a potential 'gold mine' for advertisers. By tracking user movements and other physiological signs, advertisers can know everything from the fitness level to the user's mood on that particular day. (Tracking VR emotions is also a concern).

Physical environment

VR devices can also collect information about the user's physical environment using both motion and camera data, as well as other sensors (in some cases). This can be a big security issue, but it also carries more risks than privacy. Not sure if companies collect and use this information to advertise, but hackers can use them to get more information about someone.

Virtual environment

Security issues can be compromised by bringing users into a virtual environment similar to those used (VR phishing) and privacy as well. How users shape and interact with the virtual world can be a great source of information about behavior and even conversations with other people theoretically can be run through automated language processing software. course and used more like data.

Never use a VR headset is it safer?

VR and AR are great technologies, which can turn the world into a nice, more interesting place. But that also means that anyone who wants to own this technology should know the risks and make a wise choice about the technology solutions and policies they spend on their purchases and where they will go. use them.

As with any technology, good is often accompanied by some bad things, and in this case, the bad thing is that you will create a lot of personal data, which can be handled effectively to whom that can learn more about you, thanks to AI. Network security issues have so far been far more documented than online privacy advances and that trend will likely continue with AR / VR. Hope everything will be solved before virtual reality technologies and augmented reality really become popular in life!