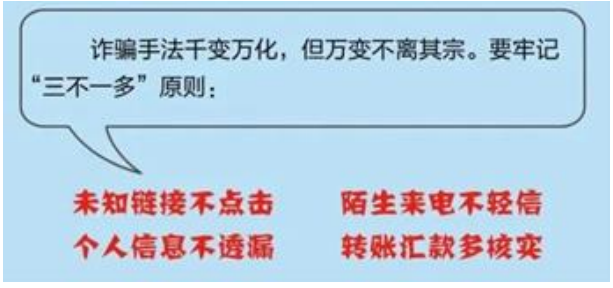
Zero Trust is a kind of life wisdom

Trust is an important part of human relationships in the real world, but in the Internet world, trust can do more harm than good. Therefore, zero trust is very hot now in the cybersecurity industry, but the concept of zero trust is not proposed by the cybersecurity giants, but by John Kindervag, the former chief analyst of Forrester in 2010. The concept of zero trust is actually a kind of life wisdom. People need to have the concept of zero trust in their daily lives. Only by believing in and following the concept of zero trust can we ensure the safety of daily life.

On June 17, 2021, the Ministry of Public Security of China launched the well-crafted "Propaganda Manual for Prevention of Telecom & Internet Fraud", which introduced Internet loans, rebates for brushing bills, "killing pigs", pretending to be charger logistics customer service, pretending to be acquaintances, false investment and wealth management, false shopping, cancellation of "campus loans", and online game false transactions etc. 10 common types of telecommunication and Internet fraud, analyzed typical cases, exposed fraud methods, and provided customized anti-fraud tips for vulnerable groups. Remind the public to keep their minds in mind and keep in mind the principle of "three Never, one Verify": Never click on unknown links, never trust unfamiliar calls, never disclose personal information, and verify more before transferring money", and beware of being frauded.

The first impression I felt after reading the brochure was Zero Trust. If zero trust is followed, people will not be frauded!



In daily life, it is not only necessary to keep in mind the concept of zero trust in preventing telecommunication and Internet fraud, but also in all aspects, then not easily hurt.

The author here lists several zero trust security related to daily life:

(1) Never trust the mobile App, if you must use it, uninstall it immediately after used. Using the App is equivalent to asking a part-time worker to do the housework. If you don't uninstall it, it equal that you allow the part-time worker to sit at home and observe all the activities in your home after finishing work. I believe that no one in the real world will let the part-time worker stay at home all the time, but everyone uses the App one time but let it on the phone for a long time.

(2) Never trust the social media moments, don't post any private information! Never post the child's photo, name, class, and other information, so as not to leak this important private information and bring opportunities to bad guy and cause harm to the child.

(3) Never trust QR codes, don't scan every QR codes! If a malicious QR code is scanned, personal privacy information may be leaked, and personal property may be lost at worst.

(4) Never trust free Wi-Fi, do not connect to any unknown Wi-Fi! Connecting to Wi-Fi means that all your Internet data is given to the Wi-Fi service provider. If the connected website does not enable https encrypted connection, your account password, mobile phone number and home address filled in online and other confidential information all have been given to the Wi-Fi provider!

(5) Never trust websites that do not display the security padlock that all browsers will display "Not secure" in the address bar. If access is necessary, do not enter any personal confidential information at these websites.

(6) Never trust links in SMS messages or emails, and never click on those links unless you can confirm that the domain name of the link is from a trusted website you are familiar with.

The author can also list many such "Never Trust". For the safety of everyone's Internet life and mobile life, we must keep in mind the concept of zero trust. Only in this way can we ensure the safety and happiness of daily life. Best wishes to everyone!

Richard Wang

Dec 21, 2021
In Shenzhen, China