Here's What Hackers Are Really Doing With Your Info

Ray Fernandez

AlyoshinE/Shutterstock
By /May 26, 2022 7:13 pm EDT

Consumers often react to the risk of being hacked in two ways: by either being extra cautious or dismissing the risk outright by saying, "It won't happen to me." Malicious intruders and cybercriminals — sometimes referred to as black hat hackers — take advantage of this popular belief for their own benefit. ESET cybersecurity advisor and industry expert Jake Moore spoke with Digital Security about the issue of lax consumer security practices, noting that many people aren't even aware of basic tools for protecting themselves like two-factor authentication.

Hackers Attack Battlefield 2042 Beta

This is a big problem because most people now rely on their personal gadgets and online accounts for accessing and storing sensitive information, including everything from health records to financial documents and work materials. Failing to update laptops and smartphones with the latest security fixes, using public Wi-Fi networks without a VPN, and using the same password for every online account are all habits that leave consumers vulnerable to hackers.

What are hackers after?

Song_about_summer/Shutterstock

F1 Solutions explains what hackers are really doing with your data: selling it, exposing it, holding it for ransom, mining it for valuable info like credit card numbers, using it for other hacks, or simply showing it off. Some hacks have nothing to do with money; instead, the attackers are out for revenge. Others

hack into "unhackable" systems or organizations just to show off or leak data in retaliation for something.

However, most cybercriminals are out for financial gain, and stolen data can contain valuable information. From credentials to credit cards and social security numbers, everything today is stored online. Hacked data is also sold in bulk on the dark web. F1 Solutions says social security numbers can sell for as low as $1, credit or debit cards from 50 cents to $1 per card (they're often sold in bundles), and Paypal credentials can be worth as much as $200. Driver licenses, digital and physical passports, and even medical information are also sold online.

Ransomware, meanwhile, is a growing trend where hackers usually target small and medium organizations, take control of their systems and data, and then offer the company the chance of recovering their computers once a ransom is paid. Given the rise of blockchain technology, it's also not surprising to learn that digital wallet credentials and credentials to NFTs sites are also increasingly stolen. Finally, data can be used to steal identities, commit fraud, do more hacking, and even vandalize websites.

Cyberattacks are on the rise

Skorzewiak/Shutterstock

SonicWall, a global leader in security intelligence, revealed in its 2022 SonicWall Cyber Threat Report that 2021 saw more than 623 million ransomware attacks globally; this represents an astounding 105% increase over the previous year. The report adds that all forms of cyberattacks are on the rise. Cryptojacking was registered to be at an all-time high with 97.1 million attacks, for example, while ransomware in the U.S. increased by 98% and in the U.K. by 227%.

There are many reasons why cyberattacks have been rising exponentially since 2020. The global pandemic accelerated a digital transformation and the entire world went online to live and work. Add that to the rise of the cloud, the new digital economy with digital assets like cryptocurrencies and NFTs, and it's easy to see why cybercrimes are on the rise. Hacking trends dominating the new era include phishing, ransomware, zero-click attacks, romance scams, and health or COVID-related scams; they affect the average

consumer, as well as small and big companies alike.

How to keep your data safe from hackers

PopTika/Shutterstock

There is no one-size-fits-all solution when it comes to digital security. Even the most advanced systems have vulnerabilities and hackers can be very sophisticated in their techniques. However, most cybercriminal attacks can be avoided by simply taking hackers seriously and believing that these hacks can happen to you, too. Using strong passwords and keeping two-factor authentication (2FA) active can prevent 90% of attacks, according to Info Security Magazine.

Other simple actions like using a trusted and efficient antivirus and keeping your devices updated can also help deter attacks. One of the most effective methods hackers use to target victims is simply asking for their passwords or sensitive information. Victims may be contacted over email, SMS,

Instagram, on scam websites, and even by phone. Cybercriminals often present themselves as agents or representatives of an organization to deceive victims and trick them into handing over their data. Many users believe that smartphones are not targeted by hackers, but that's not true — in fact, cybersecurity firm Zimperium revealed that there were more than 10 million mobile devices across 214 countries targeted by cybercriminals in 2021.

Regarding digital wallets and sites where digital assets like NFTs are stored, these are being increasingly targeted due to their vulnerabilities and the rich potential they have for criminals. Portion explains that the safest way to store your crypto or NFTs is using an offline wallet, also known as a cold wallet. If a user decides against using an offline wallet, the recommended practice is to choose a trusted online digital wallet that offers effective security measures and to always act with caution when doing P2P transactions.