EINPRESSWIRE

5 ways cybercriminals steal credit card details

DUBAI , DUBAI, UNITED ARAB EMIRATES, June 30, 2022 /EINPresswire.com/ -- Phil Muncaster, guest writer at ESET discusses some of the most common ways hackers can get hold of other people's credit card data – and how you can keep yours safe

The cybercrime underground is a well-oiled machine worth trillions of dollars annually. On dark web sites hidden from law enforcers and most consumers, cybercriminals buy and sell huge quantities of stolen data as well as the hacking tools needed to obtain them. There are thought to be as many as 24 billion illegally obtained usernames and passwords currently circulating on such sites, for example. Among the most sought-after is fresh card data, which is then bought in bulk by fraudsters to commit follow-on identity fraud.

In countries that have implemented chip and PIN (also known as EMV) systems, it's challenging to turn this data into cloned cards. So most commonly it's used online in card-not-present (CNP) attacks. Fraudsters could use it to buy luxury items for onward sale, or potentially they could buy gift cards in bulk – another popular way to launder illicitly obtained funds. The scale of the market in these cards is difficult to estimate. But the administrators of the world's largest underground marketplace recently retired after making an estimated US$358m.

With that in mind, here are 5 of the most common ways hackers could get hold of your credit card data – and how to stop them:

1. Phishing
Phishing is one of the most popular techniques for cybercriminals to steal data. At its simplest, it's a con trick in which the hacker masquerades as a legitimate entity (e.g., a bank, an e-commerce provider or a tech firm) to trick you into divulging your personal details, or unwittingly downloading malware. They often encourage users to click on a link or open an attachment. Sometimes doing so takes the user to a phishing page – where you'll be encouraged

to enter personal and financial information. Phishing is said to have hit an all-time high in Q1 2022.

These scams have evolved in recent years. Instead of an email, today you may receive a malicious text (SMS) from a hacker pretending to be a delivery company, a government agency or another trusted organization. Scammers may even call you up, again pretending to be a trusted source, with the aim of obtaining your card details. SMS phishing (smishing) more than doubled year-on-year in 2021, while voice phishing (vishing) also surged, according to one estimate.

2. Malware

The cybercrime underground is a huge marketplace, not just for data but also malware. Different types of malicious code have been designed over the years to steal information. Some record your keystrokes – for example as you're typing in card details on an e-commerce or banking site. How do the bad guys get these tools on your machine?

Phishing emails or texts are a popular method. Malicious online ads are another. In other cases, they may compromise popular websites and wait for users to visit them. Drive-by-download malware of this sort installs as soon as you visit the compromised site. Info-stealing malware is also often hidden inside legitimate-looking but malicious mobile apps.

3. Digital skimming

Sometimes hackers also install malware on the payment pages of e-commerce sites. These are invisible to the user, but will skim your card details as they are entered. There's not much users can do to stay safe, aside from shopping only with big-name brands and websites, which are likely to be more secure. Detections of digital skimming (aka online card skimming) rose 150% between May and November 2021.

4. Data breaches

Sometimes card details are stolen direct from the companies you do business with. It could be a healthcare provider, an e-commerce store or a travel company. This is a more cost-effective way to do things from the hacker's perspective, because in one attack they get access to a huge trove of data.

On the other hand, with phishing campaigns, they have to steal from individuals one-by-one –although these attacks are usually automated. The bad news is that 2021 was a record year for data breaches in the US.

5. Public Wi-Fi

When you're out and about it can be tempting to surf the web for free on public Wi-Fi hotspots – in airports, hotels, cafes and other shared spaces. Even if you have to pay to join the network, it may not be safe if hackers have done the same. They can use this access to spy on your details as you enter them.

How to keep your credit card details safe
Fortunately, there are plenty of ways to mitigate the risk of your card data getting into the wrong hands. Consider the following as a good place to start:

- Be alert: never reply to, click on links in or open attachments from unsolicited emails. They could be booby-trapped with malware. Or they could take you to legitimate-looking phishing pages where you'll be encouraged to enter your details.
- Don't divulge any details over the phone, even if the person at the other end sounds convincing. Ask where they're calling from and then call back that organization to check – although don't use any contact numbers they give you.
- Don't use the internet on public Wi-Fi, especially without a virtual private network. If you have to, don't do anything requiring you to input card details (i.e. online shopping).
- Don't save card details to online shopping or other sites, even though this helps to save time on future visits. This will reduce the chances of your card data being taken if that company is breached, or if your account is hijacked.
- Download anti-malware, including anti-phishing protection, from a reputable security vendor to all laptops and other devices
- Use two-factor authentication on all sensitive accounts. This reduces the chances of hackers cracking them open with stolen/phished passwords.
- Only download apps from legitimate marketplaces (Apple App Store, Google Play).
- If you're doing any shopping online, only do so on sites with HTTPS (it should display a padlock in the browser address bar next to the URL). This means there's less chance data can be intercepted.

Finally, it's good practice to keep an eye on all your bank and card accounts. If you spot any suspicious transactions, tell your bank/card provider's fraud team immediately. Some apps now allow you to "freeze" all spending on specific cards until you can ascertain whether there's been a security breach. There are plenty of ways for the bad guys to get our card details, but also lots we can do to keep them at arm's length.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/579175733