BRIT

writing the future

magecart and the risks of online fraud

We live in a world of online transactions and instant payments. The technological revolution has brought its own set of risks and vulnerabilities. Cygenta, an advanced cyber security business is well-versed in the evolving threat landscape. Richard@Cygenta, a leader in cyber security himself, shares his thoughts on how brands can protect themselves from the risks posed by Magecart attacks.

Criminals are evolving their methods for stealing our bank details

I drove onto the forecourt, put my card in the machine, entered my PIN, took out the diesel pump and started to fill my car. A little while later, I had a full tank of fuel, I was happy. The supermarket had the £50 that I'd paid them for the fuel, and they were happy. And the person who put the skimmer on the card machine attached to the petrol pump had my card details. Presumably, they were happy also.

It wasn't too many days before I had a message from my bank asking if I'd just made a purchase in a small town in the USA.

A decade or so later, the same thing is happening to millions of people worldwide, both in-person and online.

Card cloning and skimming devices are nothing new. Criminals have been stealing card details since cards have been commonly used. But over the last few decades, as card use has increased online, so have the tools used to steal them. Now, rather than inserting our cards into physical devices, we enter the details on websites and apps.

Enter Magecart – an emerging risk factor

Magecart is both a syndicate of at least seven cybercrime groups, and the name of a script designed to steal card details from unsuspecting consumers.

Attackers will either breach the website directly to insert their code or use a supply chain attack targeting third-party code running on the site. Unfortunately, many companies are not fully aware of the details of the code running on their websites and will likely also use third party code for things like checkout services. If your company didn't write its own website code in the first instance, you are very unlikely to notice if it's been edited or replaced.

Once on the site and activated, the script will capture the card details as they are entered, including the card number, the expiration date, and the CCV number before they can be encrypted and sent to the card issuer. Once these details are skimmed, they are then sent to the criminals who advertise them for sale on the dark web or use reshipping schemes to transfer purchased items.

continued

How can I protect my site?

Put simply; the attack consists of adding code to your website. So, being aware of the code running on your site is the most critical part of mitigating the risk. Identify which code is yours and which is 3rd party, then ensure that all code is audited for anything malicious. 3rd party code should only be used if it comes from reputable sources.

It's essential to have all web applications tested regularly by an external penetration testing company. This will help to expose any vulnerabilities in your site that an attacker might seek to exploit.

The security culture of your organisation is also of utmost importance. The use of strong passwords and 2-factor authentication, as well as a healthy patching routine, will hugely reduce the ability of an attacker to access your code.

What can we do as consumers?

While the onus is on the e-commerce company to secure their websites, that doesn't mean there is nothing we as consumers can do to avoid having our card details stolen, or our bank accounts emptied.

One simple step you can take is to use a form of payment that doesn't require you to enter your card details at all. Making use of something like Amazon Pay, Pay-Pal or Apple Pay, where a one-time token is used rather than your card details will protect your details from criminals.

If you do need to use a card, consider using a credit card rather than a debit card as you are more likely to be covered by your bank for fraudulent purchases once the theft is reported and your personal bank account is safe (remember, credit cards hold the bank's money, debit cards hold your money).

Keep an eye on your bank statements, and if you notice unexpected transactions, contact your bank immediately.

Keeping our money safe

Thankfully, banks are getting better and better at stopping this kind of fraud from targeting our bank accounts. More often than not, the first you'll hear about your details being stolen will be a message or call from your bank checking with you before a withdrawal or transaction is confirmed.

If you receive one of those messages or calls asking you to confirm or reject a payment, don't click the link or ring the number in the message. Instead, call the number on the back of your bank card, visit the bank or the bank's website directly. Scammers will often use messages like these for phishing scams where they'll direct you to a fake bank site and ask you to enter your bank details.

While the scammers might have evolved their methods, the means of protection has evolved too. Find out more about how Brit can help to protect your clients from this nefarious activity on our Cyber page.