Keep your IBAN secret, it could be easily abused

Your IBAN could be used by anyone to shop online – we successfully bought items for free on Amazon!

Our security experts recently discovered a simple but critical flaw in the payment process of some of the major online shops. Among credit cards and other secure payment methods, **they allow their customers to pay by simply providing an IBAN account number. No password, no Digipass, or none other authentication method are required.** How it works is that the money is automatically debited from the provided IBAN account number and the shopped items are delivered.

We have successfully tried this on Amazon.de, but the same process could have been applied to other major online shops as well (e.g. thomascook.com, zalando.de, eventbrite.de).

- First, we have created a dummy account, using a fake name and a randomly created email address. Then, we shopped a few items for a relatively high amount, up to 200 euros.
- During checkout, we provided the IBAN number of a random colleague and gave Amazon a fake name when they asked for the account holder's name.
- The payment was immediately accepted, and the items were shipped and delivered a few days later.

Although we delivered the items to our firm official address, to make the purchase fully anonymous, we could have used an alternative which is "Amazon Locker". Amazon lockers are self-service boxes found in public places (like railway stations) where Amazon can deliver your packages. Once delivered, the customer receives a code that can be used to unlock the locker. **Using this delivery option makes the purchase fully anonymous**. Under no circumstances, you must not reveal your identity which makes the crime perfectly legal for robbers.

This ease of use for IBAN numbers is extremely problematic. IBAN numbers are not considered as a secret at all; we often communicate them to other people and they are often shown by banks when we carry out bank transfer. Worst case, publishing the IBAN is sometimes a legal obligation (for instance with European cross-border invoicing, companies must advertise their IBAN numbers).

How is this possible?

When discovering this flaw, many of our colleagues were astonished. How would these online shops are allowed to withdraw money from any account without any consent of the account's holder?

This has been made possible thanks to the SEPA Direct Debit system. Introduced in 2009 as a new standard in 34 European countries, it allows merchants to withdraw money from any accounts, if, and only if, they have a valid mandate signed by the account's holder to do so. Direct debits are typically used for recurring payments, where the payment amounts vary from one payment to another (e.g. phone bill, energy bills, magazine subscriptions, etc.)

Direct Debits are not new in the history of the payment systems; they have existed way before to the SEPA standard. What's new with the SEPA Direct Debit is that it has changed the way mandates were obtained. Prior to SEPA, the customer was in charge to contact his bank and grant the merchant access to his account. In this scheme, the merchant had to wait for the customer to establish the mandate before he could start withdrawing money. As this could take some time and "friction" the customer, SEPA decided to simplify the process by reversing the responsibility of creating the mandate. In the SEPA Direct Debit scheme, it is the merchant that is responsible to obtain a signed mandate from the customer. SEPA is very precise about the definition of a "valid" mandate. It is a paper or electronic document that must contain certain information, explain the purpose of the mandate and must be signed by the customer. Once the mandate is done, the merchant can immediately start withdrawing money from the customer's account. As the bank will assume the mandates exist, it will not double check if the mandate exists or ask the customer to approve withdrawals. Only in case of dispute, the bank will ask the merchant to present the mandate.

This reversed scheme is obviously dangerous, as a malicious merchant could easily pretend to the banks it has a mandate while it does not. To protect the customer against potential fraud, SEPA has establish some easy refund principles. In case of unauthorized transaction (i.e. the merchant fails to show a valid mandate), the customer can request for a refund up to 13 months after the direct debit.

As we can see, SEPA Direct Debit are an easy way for merchants to obtain money. This is what the major online shops are using to withdraw money from any account. The major problem is that they do not have a valid mandate to do so. They are not strongly identifying their customer and they are not gathering legal signature to certify the mandate. **As a consequence, these merchants are taking a huge risk.** Should a fraudulent purchase be done, they will have to reimburse the bank without notice, as they will fail to demonstrate to the bank that they do possess a valid mandate. Until now, it seems these merchants have consciously decided to accept this risk.

As we can see, customers seem to be well protected. SEPA has indeed anticipated frauds by providing strong protection mechanism to the customers. **But, it has missed one important point: customer negligence**. Although any abuse of an IBAN account number can easily be reported and followed by an immediate refund, **as a customer, we do not always appropriately check our bank statements.** We might easily miss a payment we did not initiate, especially if it comes from an online store we are used to buy stuff from. Therefore, this reality puts every customer under high risk of abuse.

This flaw is not new

Although many of us were surprised by this flaw, our discovery is not something new. This payment method is available for many years on some online shops and the trick has already been unveiled for years on the Web (yet remaining surprisingly quite confidential). Typing the right keywords on YouTube will get you many tutorial videos.

This led us to believe that these online shops are fully aware of the financial risk they are taking. And that they are weighting the losses resulting of frauds against the profit of offering a convenient payment method.

The need for an improved secured process

Customers should not suffer from potential malicious withdrawal from their account**.** Therefore, we strongly believe that **the Direct Debit payment process should be more secure**.

- In particular, merchants should ensure they obtain real mandates. **With today's technologies, it could be easily done**. More and more digital identity and signature services are available that aim to strongly identify digital customers and offer qualified signature that cannot be repudiated (for instance, in Belgium we have the itsme® application).

An example of a more securely implemented process to obtain mandates is given by the company *Digiteal*. They provide an e-invoicing and e-payment solution that relies on SEPA Direct Debit to perform transactions. Unlike Amazon, Digiteal ensures the customers are properly identified through a bank-grade onboarding process (one of their solution relies on reading the Belgian eID card chip). Besides, they also check whether or not the customer has access to the bank account on which the mandate will be created (one of their solution is to send one cent on the customer's bank account along with a validation code).

- Not only merchants should implement stronger mandate creation, but also, we believe that SEPA should enforce requirements in a rule book. To avoid merchants accepting the risk and

deporting part of it to the customers. SEPA should require that the merchant's bank check the merchant's process of getting mandates before allowing it to perform SEPA Direct Debit.

- Customers' banks should also play their part. Whenever a new mandate is created on an account, they could immediately warn the customer and ask him to approve of refuse the mandate. With today's mobile apps, this scenario is certainly not that difficult to implement.

The SEPA standards have enabled more banking convergence in the EU. Thanks to those standards, it is very easy and inexpensive to make cross-border payments within EU's Digital Single Market. It is our collective responsibility to improve them for everyone's benefit and security.

Meanwhile, how can customers protect themselves?

As a customer, there are multiple ways which you can follow to protect yourself.

- First, the simplest – yet not the easiest – is to **regularly check your bank statement** in search for fraudulent withdrawals.
- Second, **some banks offer the ability to block SEPA Direct Debit**. Either totally (any Direct Debit request to your account will be refused), or by explicitly white listing third-party accounts that are allowed to withdraw money from your account. Please check with your bank to see what are the possibilities.

How companies could avoid such flaws in their processes?

As our finding demonstrates, hacking a digital system does not always rely on technical issues and does not require super high hacking skills**. In this case – and as we see that many times at our customers – the flaw is in the process itself and in its responsibilities that are not well enforced.**

While looking at the security of a system, it is very important to look at every aspect of it and not only concentrating to the technical. This includes, but not limited to, the procedural, the governance, the legal, the sourcing aspects.

This is the reason why, at Approach, we have developed skills that cover all these aspects and the whole chain of information security. Read more on our website (www.approach.be) or contact our experts to know more.

About Approach

Founded in 2001, Approach Belgium NV/SA is a consulting firm specializing in cybersecurity and development services for business and public customers. Approach provides services and solutions covering the entire cybersecurity value chain, from governance and strategy to resilient technical designs, architectures and on to implementation. Thanks to our own software factory, we are uniquely positioned to develop highly secure solutions for our clients.

For more information and our vision, or to find out more about our services, please visit our website: www.approach.be

For more information about this story, please contact:

Pierre Alexis, Cyber Security Consultant
+32 485 91 40 60 | pierre.alexis@approach.be
Axis Park – Rue Edouard Belin 7 – 1435 Mont-Saint-Guibert – Belgique

Our partner, Digiteal

This article has been written with the technical advisory of Digiteal, a company specialized in payment processing using SEPA Direct Debit.

By making it accessible to secure money in Europe, Digiteal creates trust between a buyer and a seller. By optimizing invoice management and payment, Digiteal avoids the ecological waste of paper invoices. All this allows companies and individuals to have a positive impact on the environment and to devote their time to what is essential.

For more information, please visit our website: www.digiteal.eu.