We are more accustomed to access all our digital accounts on the cell phone now.

Not only email, Twitter or Facebook, but also our bank account and those that allow access to the files we store in the cloud and use many other online services. This makes our smartphones an attractive booty for hackers, who seek access to those accounts to steal sensitive information, such as passport details, confidential documents, and money.

And just with your telephone number and some ingenuity and "social engineering" (manipulation techniques used by computer criminals) hackers can easily convince the customer service of our operator that the number belongs to them (and not you).

The Way You Pick up the Phone Can Make You Vulnerable to Hackers

Here are the latest trends in hacking, although cyber criminals have been doing it for quite a while.

2-Step Verification

Hackers usually start by obtaining information that we make available on the internet: your name, address, birthday. Then when they obtain your number, they can convince the operator of the telephone company that the number is theirs.

Many only need to click on the option "I forgot the password" to sneak into your account, without you being able to do anything about it. If the hackers succeed at this stage, and have managed to circumvent the measures of the teleoperator, they can access your accounts without a problem.

+44 20 7183 5820

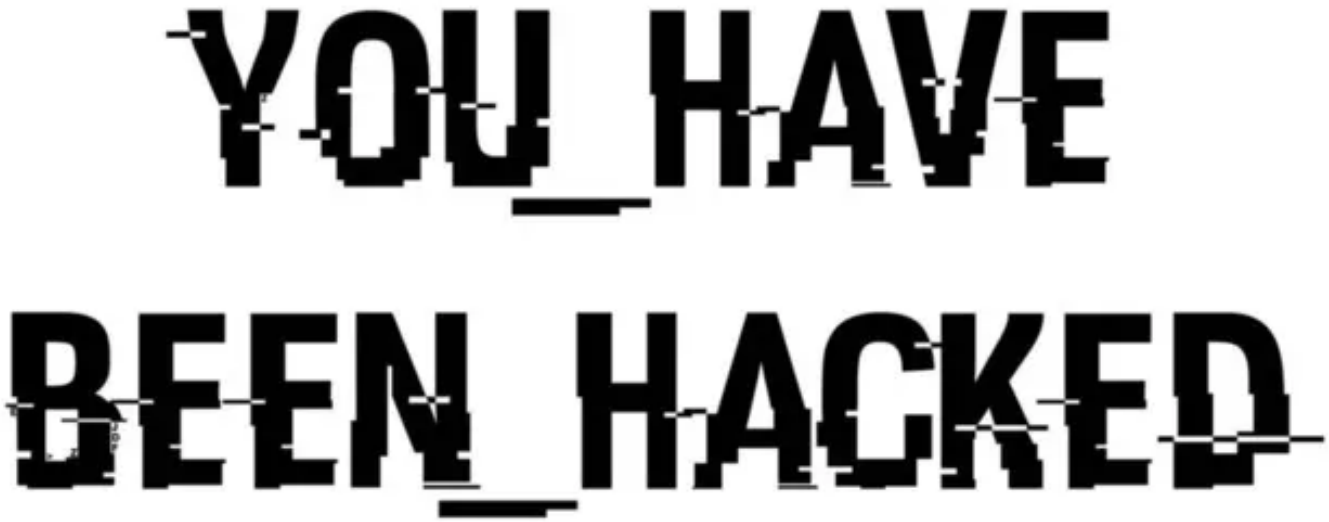
info@magora.co.uk
sales@magora.co.uk

For this they take advantage of the so-called "two-step verification systems" that work through SMS and send codes to clients to - paradoxically - secure more accounts against fraudsters.

- The fact that your phone number is used as a guarantee system to protect it can become a great opportunity for hackers.
- Crypto technology specialists reported that in recent months many hackers have used this technique to steal virtual money (Bitcoin, Ether and other cryptones).

But this crime can be perpetrated by anyone who uses the most common web services: Gmail, iCloud, Facebook, Internet banking, PayPal, Dropbox and many others. And a recent investigation by the New York Times confirms it: more and more reports of hackers calling telephone signatures, pretending to be the users of the number or cell in question.

How to Detect If Your Computer Was Hacked and What to Do About It?



It is important that you, as a user, look for ways to protect your numbers and keep them safe from the clutches of scammers.

1. **Set an access key**

   It is the most basic precautionary form, although it could also be hacked, so take extra precaution.

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

2. **Use a specific email address**

   Most likely, you'll use the same email address and phone number to access all your accounts. The best thing to be protected is to use different accounts. You need at least three: the main, the phone, and sensitive accounts (bank, Facebook or Dropbox, for example). This way you will give less options to hackers.

3. **Strengthen security requirements**

   For example, you can tell your telephone operator that you just want to make changes to your account in person or by submitting a photocopy of your identity document.

4. **Disable online access with your carrier**

   This option is somewhat more radical and can be annoying in some cases, but it is most effective to prevent hackers from taking advantage of potential vulnerabilities.

5. **Try Google Voice**

   When you sign up for a Google Voice account you can block the number and manage and process your call history, in addition to text messages and conversations, among other things.

6. **Use strong passwords**

   This is the universal advice for everything that has to do with digital technology: the more complicated your password, the better.

7. **Do not connect your phone number to sensitive accounts**

   Avoid linking your number with Facebook, your bank account and other online services. It is the safest option to avoid fraud.

8. **Keep your computer updated**

   By regularly updating your computer, you block attackers from being able to take advantage of software vulnerabilities that they could otherwise use to break into your system.

9. **Make sure your computer is configured securely**

   A new computer these days should have security controls in place, often promoting you with questions, such as “This may not be safe, you sure you want to download?” You are downloading from a third party source...etc”

   However it is recommended to make sure that you pay attention to security settings.

10. **Be careful of linking accounts**

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

Although convenient, sometimes signing in using Twitter or Facebook, might make you more vulnerable, by exposing data to cyber-criminals.

Our expert team advice: keep to these 10 simple, but useful rules and your will be protected from the hacker, better than 75% of the world smartphone users.

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk