next I.T.
technology solutions
that make business sense

Who’s Snooping on your online business transactions?

Did you know that cyber criminals can break into your banking information in just 36 hours? And, that they can be gone with your money and all your personal details before you even know it?

A journalist group in the UK hired some ethical hackers and gave them the challenge to hack into one of their banking accounts. They wanted to see how long it would take to do this. It took only 36 hours. And, believe it or not, all the hacker needed was their name!

This is what they did:

- The ethical hacker had the volunteer's name
- They searched on social media for more details about him (including friends and family member's names, etc.)
- Then, they logged into lower-priority websites (like eBay and hotel-booking sites, etc.) to gain his address, credit card numbers and phone number
- With just this information, they could then hack into his other accounts and websites!

So, How Can You Protect Yourself?

Here Are Some TIPS to keep your Banking Information Safe & Secure.

Use Better Passwords.

- Just like you make sure that the key to your house isn’t easy to find, make sure your passwords aren’t easy to crack.
- Ask your bank about using two-factor authentication. When you want to access your account online, your bank will send you a code via email or text message to authenticate that you’re the owner of your account. You’ll only have a short period of time to use the authentication code, along with your password, to enter your account online.
- Avoid using elements of your name, address, or birthday in your password.
- Don’t use the same passwords across different sites and applications.
- Try developing “Password Phrases” for example: HELLO@Isitmeyouarelookingfor?

Consider Using a Password Manager.

- Most password managers save and generate secure passwords for you, meaning you only have to remember one password — the one that opens your vault.
- There are free password managers, and paid ones. They all have different features and benefits. But they all generate complex passwords.

Keep All Your Systems Up to Date.

- Software companies are always developing updates to improve security. Make sure you download and install these updates.
- Put a tickler in your calendar to manually update your passwords once a month at the very least.
- Or even better, set your computer to authorize automatic updates.
- You should still regularly check your system to ensure everything is up to date in case malware was accidentally downloaded.

Beware of Sneaky Activities.

There are often clues that someone’s trying to access your info.

- Look into password/account access emails if you don’t recall an interaction — For example, if you received an email you didn’t ask for, such as a survey for a service you didn’t use, or asking if you got a package you didn’t order.
- Be wary of any phone calls or emails from your financial institution or PayPal saying there’s something wrong with your account, and asking you to disclose information.
- Never click on a link to a bank URL. To make sure you’re at the right URL, you’ll note that there’s a lock icon indicating it’s secure. Always just type in the URL for your account. Don’t even trust your “favorites.” There’s now a malware that can get into these!

Set Up as Many “Walls” as Possible.

The more protection around your information, the safer it will be.

- Consider setting up a Firewall. This is a barrier or shield that’s intended to protect your PC, Tablet, or phone from the data-based malware dangers that exist on the Internet. It can be a physical one that’s attached to your router.
- Consider setting up a Virtual Private Network (VPN). This is a group of computers networked together over a public network that shields information about where you are, and what you’re doing online. Your VPN could be anywhere (England, Africa, Brazil) and people will think you’re working from one of these locations instead of where you are.

Use Common Sense

If you make it easy for others to access your information — They will!

- Don't write down passwords, anywhere! — Not even in notepads on your phone.
- Update your passwords regularly. This is very important.
- Never access secure sites on public computers. Someone may have installed malicious software on the computer to capture your password. Or, someone can go into the cache to get your information.
- Notify your bank of any phishing activities/emails.

Bonus Tips

- When doing online banking on your phone, turn off the WIFI and complete your transaction using the cellular network instead — Especially if you're out and about. It's much harder for hackers to crack this network.
- Make sure your Bluetooth is OFF on all your devices unless you're using it. If it's on all the time, it's easier to access your computer or phone.
- Be cautious about posting photos or details about your home, family or vacations on social media. You may be telling hackers or thieves where you are (that you're not home), what you're doing, or unknowingly providing information about family members they wouldn't want to share.
- Make sure your antivirus protects your system from the latest ransomware. Ransomware can come from accessing websites or downloads, etc.

Protect yourself and your business from online thieves. For more information, contact the team at 866.388.6398 or www.next-it.net.