accessnow.org

TOP 10 TIPS TO PROTECT YOUR SAFETY AND IDENTITY ONLINE

We live in the age of information sharing. Social media sites, IM clients, and other web services enable to people engage in discussions, organize events and even raise awareness about the issues they care about. But what if that information gets into the wrong hands?

The power of the Internet is also its weakness. One compromised account can trigger a domino effect: once a hacker gains access into your account, they can break into your other accounts, and your friends' accounts too.

The best step is prevention. In order to protect yourself and your friends, you have to secure yourself by (1) protecting your computer and (2) securing your online accounts.

PROTECT YOUR COMPUTER

Taking these steps go a long way towards protecting you from viruses and other malicious programs that can be used to steal your passwords and other private information.

1. Keep your computer up to date

Make sure you keep your operating system is up to date, whether it be Windows, Mac or Linux, up to date!

Instructions: Mac, Windows

2. Keep your antivirus definitions up to date

The same thing goes for your antivirus software. New threats are emerging all the time, but in order to catch them before you become infected, your antivirus software needs to be current with the latest updates.

If you don't have an antivirus software currently, there are some options that are available for free over the Internet:

AVG
Avira

3. Install anti-spyware

Spyware is malicious software that can be used to monitor your activity while you are on your computer. It can also be used to collect passwords and other personal information.

Most paid anti-virus softwares include anti-spyware, but there are free packages available. You should make sure you have Spybot and an ad-blocker, like Ad-aware, installed.

PROTECT YOUR ONLINE ACCOUNTS

The Internet is the link between your computer and your identity. Here are some basic steps you can take to protect your privacy and security online:

4. Make strong passwords.

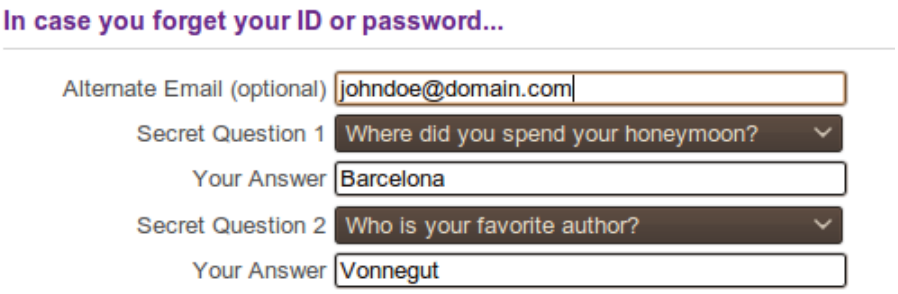
Most people do not make strong passwords because they are worried they will forget it or misplace it. Google offers a good way to make a strong password that you can easily remember. Watch it here: http://www.youtube.com/watch?v=aOqkGmZ4p-s&feature=channel

DO's	DONT's
• A combination of capital and lower case letters • Numbers • Special characters • It should be easy for you to remember, but difficult for others to guess. • The longer the password, the better!	• complete words, e.g. browndog • Private Information about yourself or your family • Publicly available information about yourself • sequential numbers, e.g. 1234 • repeating numbers, e.g. 333 • any combination thereof
example: uW6&tZ	example: browndog1234

5. Choose your secret question carefully.

Secret questions are used by some sites to prevent hackers who attempt to gain access into your account through password resets.

When picking your secret question, make sure the answer cannot be found by looking at your social media profile or blogs. For example, using the question "Where did I spend my honeymoon?" may not be a good idea if your Flickr account is filled with pictures of you with your spouse in Barcelona.



6. Recognize phishing attempts

Hackers often try steal passwords by baiting people into visiting fake websites disguised as legitimate ones, usually a bank. Their goal is to encourage you to enter your username and password into the fake website.

Some basic guidelines to avoid phishing:

- Manually go to websites that ask for passwords, personal information, etc by typing their address into your browser.
- Always look at the address bar to make sure the website domain (http://www.google.com) is spelled correctly.
- Use a browser that includes phishing filters. We recommend Mozilla Firefox, Google Chrome and Mac Safari.
- Always check suspicious links from your email, chats and IM before you click on them. Right-click and select "View Link Location" from the drop down menu.

How to recognize phishing:

- Sites designed to trick people into phishing scams often have mispelled URLs designed to look like the original. For example, gmail.com may be written as gmaiil.com.
- If an email from an official looking business asks for your password or other personal information, it is most likely a phishing scam.

7. Do not use the same username and password for every site.

Most of us prefer ease and convenience, so we use the same user name and password across different sites. If a hacker gets into our Facebook using our password, he can figure out what our email address and birthday is.

You don't have to create a different username and password for each account, but it is good to have different user names and passwords for a few main sites where you have important information.

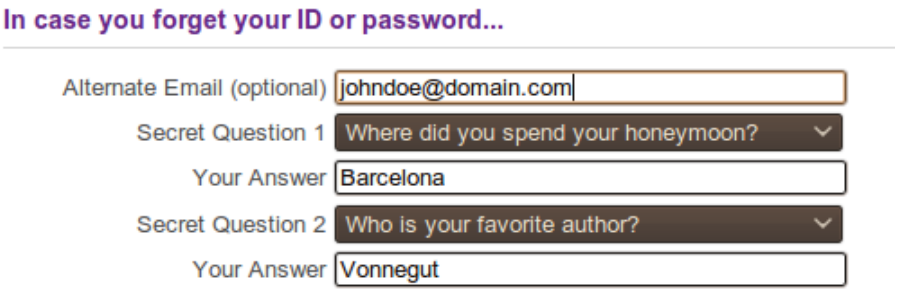
A good suggestion is to create different types of passwords for different types of accounts based on their security level.

For example, your password for your email or websites that deal with financial issues and credit card information or other confidential information should be longer and more complex.

8. Be careful about what information you make available to others online

Hackers don't need to infect you with a virus in order to break into your account – sometimes they can find exactly what they need by looking at your Facebook profile or doing a Google search.

Remember those '25 Random Things' on Facebook, where you talked about how you met your favorite author in person? That also happens to be a commonly used secret question:



Therefore, it is important to be aware of what you make available on sites like Twitter, or what your friends post about you.

If you use social media sites like Facebook, LinkedIn, or Twitter – make sure to do the following:

- Control the privacy settings. Facebook's privacy guide can be found here.
- Be aware of what information those sites make publicly available. View your public profile from time to time, which is usually accessible through the site's privacy settings.

Important: No matter what site you are on, never make your birthdate publicly available.

If your friends post information about you, be sure not to use that information in any of your accounts. For example, a friend of yours might have a Facebook event listing for your birthday that is available for the entire community to see. Knowing this, none of your passwords or usernames should contain your birthdate, or your birthyear.

9. Use encrypted logins whenever possible.

Unfortunately, most sites transmit your password in plain text by default, making it easy for hackers to steal your password.

Use encrypted login pages whenever possible – they transmit your password in gibberish over the Internet, making it difficult for hackers to steal your password.

Encrypted login pages look like this:

https://twitter.com instead of http://twitter.com (notice the extra bolded 's' in http)

10. Encrypt your communications (Chat, IM, Skype)

In addition to passwords, you can also encrypt our communications. There are some very simple to use programs to encrypt your online communications. They ensure when you are chatting with someone, what you tell them is transmitted in gibberish that only your friend's computer can understand.

Skype has encryption built in and is a simple solution. But if all of your friends prefer Google Talk, AIM, MSN, or Yahoo, there are options available as well:

- For Windows and Linux: Install Pidgin and the Off the Record plug-in.
  Instructions: Windows Linux
- For Mac: Install Adium and enable the Off the Record plugin.
  Instructions: Mac

Caution: Google Chat over a browser like Firefox allows you to enable "Off the Record", but it is not the same. All it does is remove the logs of your chat from your email so your conversation will not be archived if the option is enabled. It does not transfer your chats in gibberish, making it possible for hackers to read what you are saying.

AND REMEMBER: Educate your friends!

One hacked Facebook account puts every one in that circle of friends at risk. Hackers depend on the connectivity of the Internet to achieve their goals in the same way we depend on the Internet to share information.

With how interconnected we are, it is absolutely necessary to encourage your friends to secure themselves. Forward this guide along to get them started.

More technical solutions can be found on the following guides.

Protektor Manual:(Mac, Windows , Linux)
Security in a Box

Last revision: June 12, 2010