The Essential Security Risk Assessment Checklist

to Improve Your Online Protection

How protected are you against cyber attacks?

Do you know what makes you vulnerable to hackers?

What could you do to strengthen your defenses?

We want to help you map your personal digital assets and see where you stand in terms of cyber security. Answer the following questions and find useful information security tips at the bottom.

1. What type of information do you have stored on your computer (pictures, work documents, applications, passwords, etc.)?

You can list:

Personal information (pictures, passwords, financial information, emails, insurance policy details, etc.)

Professional data (work documents, authentication details for work applications, confidential conversations and corporate data, etc.).

Also, make sure to list what you have stored both locally, on your computer, and in the cloud (Dropbox, Google Drive, OneDrive, etc.).

2. Which online services do you use more often?

Here are some of the most commonly used online services you can list:

Email, Search engines, Online maps, Weather apps, Social networking, Online banking, Travel websites, Video streaming websites, Download portals, Chat applications, Online games, News websites, Blogs, Online music streaming, Infotainment websites, etc.

3. Define how valuable each asset to you.

You can use three degrees of importance: “**low**”, “**medium**” and “**high**”. Define this value based on the potential cost (financial, reputational or emotional) of an unauthorized person gaining access to that piece of information or service.

For example:
Online banking password – high value
Playlist stored on your music streaming service – low value

4. How do you keep your sensitive information safe?

Consider the following options (and others that apply to your situation):

I use strong passwords (longer than 8 characters and including symbols and numbers)
I use passwords for both my online accounts and for logging into my laptop/tablet/phone
I use two-step authentication whenever it’s available
I have set strong security questions in the event of a security breach
I have my email accounts connected, so I can regain access to my information in the case of a cyber attack
I set up my phone number to receive alerts from important services (such as online banking or email) in the case my accounts should be compromised.

5. What kind of security are you using?

Here are some of the security options you might be using (and should use if you're not already doing it):

Antivirus, Firewall, Malware detection and removal program, Encryption application, Pop-up blocker, Anti-spyware.

6. What security software are you using against financial and data stealing malware?

Do you have any of the following products installed?

Malicious software removal tool (on-demand anti-virus tool - "on-demand" meaning it lacks real-time protection - that scans the computer for specific widespread malware and tries to eliminate the infection)
Real-time Internet traffic scanner (this type of malware protection scans all incoming network data for malware and blocks any threats it comes across)
Malware detection and removal software (can be used solely for detection and removal of malware software that has already been installed onto a computer)
Website security scanner (such a products checks the website you want to visit, detects malware, may note outdated software, and may report known security issues).

7. Are you using a back-up solution for your operating system or for your vital information?

Do you have a back-up system in place:

Using an external drive or a cloud account (Dropbox, Google Drive, OneDrive, etc.)
Scheduled, automatic back-ups performed on a weekly basis (ideally, so you don't lose progress you've made with your work).

8. How do you protect your shared documents (e.g. Google Docs) or gadgets (computer, tablet, etc.)?

If someone else is using your devices or has access to confidential information, do you:

Set up guest accounts with limited access (for hardware devices)?
Share documents giving view-only permission?
Share documents, giving editing privileges, while maintain administrator privileges?
Keep back-up or copies of the shared documents and files that other people have access to?
Have alerts set up that would inform you if anyone would try to delete or modify important files and documents?

9. How do you manage your passwords?

Think of the following situations:

Do you have strong enough passwords (longer than 8 characters, including symbols, numbers and letters, both small and capital)?
Do you store your passwords in the browser?
Do you use a password manager application?
Do you use the same password for more than one account?
How often do you change your password?
Do you share your passwords with someone else?
Who could access your password, and, if they do, what methods can you use to regain control of your accounts (SMS alerts, security questions, two-step authentication, etc.)?

10. Do you regularly update the software you use?

Consider some of these choices:

Do you perform operating system updates when you're prompted to do so?
Do you have automatic software update set up for both your OS and your applications?
Do you regularly update Oracle Java, Adobe Reader or Adobe Flash, which are known to cause 85% of security exploits that hackers use?
Do you keep your browsers updated to the latest versions?
Do you have a security product that updates and patches software automatically?

11. Can you identify the main types of cyber attacks?

Could you recognize what kind of cyber attacks you may come against? Here are some of them:

Infectious malware (virus, computer worm)
Concealment viruses (Trojans, backdoors, rootkit, clickjacking, etc.)
Malware for profit (privacy-invasive software, adware, spyware, botnet, keystroke logging, web threats, malbot, scareware, ransomware, etc.)

The key to preventing major data leakage and minimizing the consequences of a cyber attack is to be able to detect it and know what to do about it. You can become an important asset to your own cyber security defenses if you can learn about cyber security threats and get adequate protection.

Did you find this assessment valuable?

Forward it to a friend, a family member or a co-worker who might find it useful, so they can evaluate their cyber security level. And be sure to remind them to check their results on the Heimdal Security blog:

https://heimdalsecurity.com/blog/security-risk-assessment-checklist/