




are

you

cyber

secure?



In today's Internet environment, where information flows more quickly, effectively, and freely than ever before, each of us has a key interest in – and responsibility for – ensuring the security of our information and the privacy of our communications. We can enjoy the full benefits of the Internet only if we have confidence and trust that our on line transactions and communications are private and secure.

Ensuring cyber security is an ongoing process, not a one-time fix. It requires the use of proven cyber security software and, in the case of organizations, the adoption of strong security policies and the use of trained security professionals.

There are simple steps, however, that each of us can take – whether in personal, business, or governmental settings – to improve our cyber security. BSA has developed the following checklists to help individuals, organizations, and government agencies quickly evaluate and improve their cyber security readiness.

For additional information on cyber security and BSA's efforts to create a safe and legal on line world, visit [www.bsa.org/security](http://www.bsa.org/security).

questions that  
individuals,  
organizations,  
& governments  
should ask  
themselves

## Improving the Cyber Security of Individuals

### *questions to ask...*

1. Do you have anti-virus software installed on all of your computers? Most anti-virus software includes an automatic update feature. Have you activated this feature?
2. Do you have a home firewall installed that protects your computer(s) from unauthorized access to and use by hackers?
3. Do you check for security updates at least every 30 days for all programs on your computer(s), including operating systems. Alternatively, have you enabled automatic updating and/or subscribed to a notification service provided by the vendor?
4. Do you change the passwords you use on websites and on home computer(s) every 120 days and are they strong passwords that contain numbers and symbols?
5. Do you use encryption to protect sensitive information stored on your computer(s), such as financial or medical information?

## Improving the Cyber Security of Small Organizations

### *questions to ask...*

1. Does every computer have anti-virus software installed? Most anti-virus software includes an automatic update feature. Have you activated this feature?
2. Do you have a firewall installed that protects your computers from unauthorized access to and use by hackers?
3. Do you check for security updates at least every 15 days for all programs on your computers, including operating systems or have you enabled automatic updating and/or subscribed to a notification service provided by the vendor?
4. Do you change computer passwords every 120 days and are they strong passwords that contain numbers and symbols?
5. Do you use encryption to protect sensitive customer and business information stored on your computers, such as credit card data, company business plans, and payroll information?
6. Do you use backup software and do you keep a recent (1 week old or less) backup offsite?
7. Do you have at least one employee or outside consultant responsible for your cyber security needs and does he or she have a complete understanding of your unique system needs and design? Do you budget for the purchase of computer security tools?
8. Do you talk to your employees about the need to be cyber secure?
9. Do you have insurance coverage for cyber crimes and is the coverage adequate to compensate you for potential losses?
10. Do you report cyber attacks to local law enforcement agencies and to your IT provider?

## Improving the Cyber Security of Mid-to-Large Organizations

*questions to ask...*

1. Does every computer have anti-virus software installed? Has the IT manager enabled any automatic updating feature in the software?
2. Does every network use a firewall to prevent unauthorized access to and use by hackers? Are the firewall rules and settings current and limited in order to only allow necessary data transfers?
3. Does your IT administrator check for security updates at least every 7 days for all programs on your organization's computers including operating systems? Alternatively, has your IT administrator enabled automatic updating and/or subscribed to a notification service provided by the vendor?
4. Are computer passwords changed every 90 days and are they strong passwords that contain multiple numbers and symbols?
5. Does your organization use end-to-end encryption to protect your sensitive customer and business information, such as credit card data, company business plans, and payroll information? Does your organization securely authenticate the electronic communications of your customers, partners, and employees?
6. Does your organization use backup software daily and keep the backup offsite? Alternatively, do you use an on line backup service?
7. Does your organization have at least one employee or outside consultant responsible for your cyber security needs and does he or she have a complete understanding of your unique needs and system design? Does your organization's annual budget planning process include a specific computer security component?
8. Does your organization explain to all employees on a regular basis the need to be cyber secure?
9. Does your organization have insurance against cyber crime and is the coverage adequate to compensate you for potential harms?
10. Does your organization have a central person to coordinate reporting of cyber attacks to local law enforcement agencies, your organization's IT provider, and, as appropriate, share that information with other relevant organizations?
11. Does your organization's IT staff have basic security training and is there a cyber security plan in place that is developed and administered by senior IT staff?
12. Does your organization's leadership take an active role in determining basic cyber security policies and fully understand the dangers of not being cyber secure?
13. Does your organization use virtual private networking to protect against data interception?
14. Does an outside group conduct an annual security audit of your organization and is that audit reviewed by senior management?
15. Do personnel reviews for both IT and non-IT staff within your organization include a discussion of the importance of cyber security?

# Improving the Cyber Security of Government Agencies

## *questions to ask...*

1. Does every computer have anti-virus software installed? Has automatic updating been enabled?
2. Does every computer use a firewall to prevent unauthorized access to and use by hackers? Are the firewall rules and settings current and limited to only allow necessary data transfers?
3. For all programs on your computers including operating systems, does your IT staff check for security updates daily? Alternatively, has your IT staff enabled automatic updating and/or subscribed to a notification service provided by the vendor?
4. Are computer passwords changed every 60 days and are they strong passwords that contain multiple numbers and symbols?
5. Is end-to-end encryption widely deployed throughout your agency and used to protect communications with other agencies? Does your agency securely authenticate the electronic communications of your customers, partners, vendors, and employees?
6. Does your agency use backup software daily or, in the case of highly critical data, in real time, and is the backup kept offsite? Alternatively, is an on line backup service used?
7. Does your agency have a cyber security plan that is updated and validated monthly? Does your agency's annual budget planning process include a specific computer security component?
8. Does your agency explain to all employees on a regular basis the need to be cyber secure?
9. Does your agency have an offsite contingency plan for critical government functions and communications?
10. Does your agency have a central person to coordinate reporting of cyber attacks to local law enforcement agencies, your organization's IT provider, and, as appropriate, with other organizations?
11. Do all of your agency's IT staff have basic security training and is there a cyber security plan in place that is developed and administered by senior IT staff?
12. Does your agency's leadership take an active role in determining basic security policies and fully understand the dangers of not being cyber secure?
13. Does your agency use virtual private networking to protect against data interception?
14. Does an outside group conduct an annual security audit of your organization and is that audit reviewed by senior management?
15. Do personnel reviews for both IT and non-IT staff within your organization include a discussion of the importance of cyber security?
16. Does your agency view cyber security as an enabler of e-government and integrate it into all agency e-government investments from the outset?
17. For extremely sensitive and vital information, does your agency restrict, track, and log all access to such information? Are those logs stored and reviewed periodically?
18. Has your agency fully implemented all existing government security regulations?
19. Where appropriate, does your agency use biometric security tools to control access to information?
20. Does your agency conduct background checks on all potential cyber security staff?

Never has  
the security  
of networks  
and computing  
been more  
paramount.

Business Software Alliance  
1150 18th Street, NW, Suite 700  
Washington, DC 20036  
[www.bsa.org](http://www.bsa.org)

