Legal Services National Technology Assistance Project

Helping nonprofit legal aid programs improve client services through innovative use of technology.

www.lsntap.org

10 Tips for Cyber Security

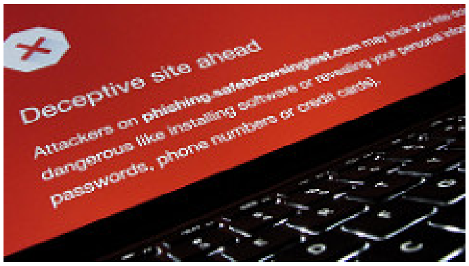
1.) Manage your Passwords

You can use a password manager like LastPass to keep all your passwords in one place. The software allows you to create and store strong passwords for all your employees and change passwords simply and easily when employees leave the organization.

Allowing your employees to choose their own passwords means that the passwords won’t be secure, and it also means that your employees are likely re-using their personal passwords for work. Re-using passwords means that if an employee’s personal account got hacked then the hackers would also have access to their work accounts since they share a password. Please see our video on The Basics of Using Lastpass.

2.) Keep your Software Up to Date

When people working for companies that build operating systems find a way to exploit the OS, or fix a security hole they make a windows update. Ensuring your system’s all are updated is the best way to keep your computers clean and infection free.



Deceptive site ahead

Attackers on phishing.safebrowsingtest.com may trick you into do

dangerous like installing software or revealing your personal info

passwords, phone numbers or credit cards).

Christiaan Colen - Flickr

3.) Beware of Public Wifi

Free public Wi-Fi networks such as those provided by cafes or hotels don’t encrypt their data traffic – so plain text, unscrambled images, and sound flying over the network are all there for enterprising hackers to intercept or collect. So passwords, financial information, and sensitive images aren’t safe.

You will need to inform your workers that when using public wi-fi they are not to log into work email unprotected, as this could compromise your system and allow access to a hacker. You can have employees use VPN's or "virtual private networks" that will allow people to securely surf the internet or use work email in public wi-fi. This becomes particularly crucial on business trips. Additionally, using extensions like "HTTPS FOREVER" will force many major websites to use more secure, encrypted connections - thus making you and your organization safer on the internet.

4.) Backups and Redundancy

Basically redundant data storage provides protection against hard drive failure rather than an actual backup of your data. Computers with critical data should have set up redundant backups in place so that in the event of a virus or malware issue your date can all be restored.

You can use services like BackupBuddy to automatically create backups of your website, which you can deploy in the case of an attack. Having Dedicated portable hard drives that regularly backup your files will add an extra layer of protection.

5.) Physical Office Security

All the antivirus software and all the backup systems in the world won’t keep your office completely free of cyber-crime as long as somebody can just walk into your office unchallenged and either pick up a post-it note with a password on it, or sit down at somebody's logged in computer. To safeguard your office consider employing somebody to watch the front door or keeping it locked. Never let your employees physically write down passwords

6.) Conduct Cyber Attack Response Tests

Don’t figure out how to deal with a cybersecurity attack AFTER it happens. Make a plan and test it. You don’t necessarily have to infect your network for a test, just tell your employees that a “virus” has infected the network and ensure everyone knows what to do in order to restore backups, change company passwords etc. Don’t just have a backup system in place for your website, TEST the backup system and ensure it works. If in performing your test your office is unable to restore backups locally, change passwords etc without a problem then when you actually have a real attack your office will be much better prepared.

7.) Teach your Office about Phishing Scams

Basically phishing is when you receive an email pretending to be from a website or financial institution that attempts to trick you into revealing your password or logging into a banking center. You might get an email that looks like it came from your bank except the url doesn’t go to bankofamerica.com it goes to something like “bankofa.com” or “bankofamerica.info” or something like that. Then when you click the link it will take you to a login page that looks just like what you are used to, so that the thieves can collect your login information.

Educate your office about how to spot phishing scams. Avoiding them can be as simple as never logging into any of your websites from links sent via email. Get an ominous email about your checking account? Pick up your phone and actually call your bank rather than clicking through in the email. We at LSNTAP would highly recommend you conduct a live training seminar where you show real phishing scams compared to real emails, so your employees can better be prepared.

8.) Review your Online Accounts and Credit Regularly

By regularly monitoring your credit and online banking institutions you can find and fix problems before they get worse than they already are. Services like karmacredit.com will allow your organization to monitor their credit in real time thus ensuring nobody has fraudulently opened any lines of credit or done any damage to your company’s credit score.

9.) Disable Bluetooth

If a bluetooth device is in the area your phone can connect to it automatically. Since bluetooth requires no password, it can be an easy way for hackers to hijack your phone or steal your password. The problem is that there are four different pairing methods for bluetooth and each of these types of Bluetooth has it’s own specific flaws and vulnerabilities.

For example "Numeric Comparison" requires a display (not all devices have one), while Just Works is vulnerable to attacks & exploits. Out-of-Band requires a separate channel for communication (not all devices support this) and Passkey Entry can be eavesdropped against (at least in its current state).

10.) Bring Your Own Device Policy

Have a strict policy for your office that if people use their personal devices for work they must have remote wipe capability set up so in the event of a laptop or cellphone being stolen with work information on it, the device can be remotely cleaned right away. Also consider mandating a particular anti-virus software (Avast! is a good one.) If you don't mandate the use of a specific antivirus software and pay for it then you can't be sure those devices are properly protected from virus and malware attacks.

©Legal Services National Technology Assistance Project