

Developing an Internet Usage & Security Policy for Your Company

The purpose of this document is to help you understand the importance of implementing and enforcing an appropriate company-wide policy for internet usage and security, as well as the key points to consider in its development. The longevity of your business depends on your ability to keep your confidential data away from prying eyes. Are you aware that in some cases, a breach to a company's security can be considered their own responsibility? For example, in law firms, such a breach can be construed as a violation of client-attorney privilege. In order to protect your company from liability and to maintain efficient workflow, it is imperative that every business develop and implement such a policy and ensure that it is strictly enforced.

Web Browsing

The web has become a vital resource for most companies, and while most legitimate corporate web sites are secure and very safe to use, there are countless web sites on the internet that are not. Because of this, personal web browsing in your office can threaten the security of your entire network. In addition to diminishing workplace productivity and lowering the overall efficiency of your network, excessive personal web browsing can open your company to a number of different security threats, including inadvertent installation of spyware, keystroke or screenshot loggers, viruses, and other malicious programs. As a result, it is common for businesses to limit or altogether prohibit personal web browsing at work. Higher-end firewalls can restrict access to specific web sites from within your network, as well as produce reports of which sites your users are accessing, when, and for how long.

Email

Email, like web browsing, has become a mainstay of business communication, but it can also mean problems for your company's network. Personal email usage in the workplace can diminish productivity and threaten your network's security. High levels of spam can lower your network's efficiency and deplete available hard drive space on the E-mail server. Even legitimate business email messages can contain viruses, worms, or other harmful program files that, if executed, can cause severe damage to your system that may not be noticed for some time. In addition, there has been a recent and continuing increase in the amount of email-based scams, including "phishing". "Phishing" scams present themselves as apparently legitimate emails, generally from a financial institution or online retailer, requesting that you visit their web site to re-enter or confirm your account information. However, the links provided lead to a site that, although it appears legitimate, serves to collect this account information (which can include bank account, credit card, or social security numbers, and other confidential data). This data is then relayed to a third party who bears no affiliation with the purported company and may use it for malicious purposes, including identity theft.

Instant Messengers

Despite its recreational origins, instant messaging (IM) has emerged as a specialized application of internet technology that bears an increasing impact on business communications. Although some companies strictly prohibit instant messenger usage, there are an increasing number of companies for whom instant messaging has become a vital means of both intra-office and inter-office communication.

Some of the dangers are inherent to the design of these applications, which can provide a “back door” through existing network security measures, leaving your company vulnerable to hackers. In addition, many instant messaging applications provide file sharing capabilities, which if used improperly can allow outside access to your company’s confidential documents and data. In addition, industry experts have warned that we may very soon see outbreaks of viruses specifically designed to target instant messaging applications. For law firms and other businesses who deal with confidential client information, it is important to understand that most instant messaging programs offer limited, if any, logging capabilities, which means that although important information can easily be transmitted via instant messages, it may be impossible to trace. Whether or not you choose to allow instant messaging in your organization, it is crucial that you understand the risks associated with them and develop a formal, company-wide policy on their usage.

Program Downloading & Installation

Unauthorized downloading and installation of software from the internet can pose several important threats to your company’s network security. Most significantly, installation programs are downloaded in the form of “executable” files, meaning that they contain a program that is activated by double-clicking. Any executable file can contain viruses, spyware, keystroke loggers, or other malicious programs. Executables downloaded from the internet are particularly dangerous, since it can be difficult to determine their origins. Even legitimate software from reliable sources (such as Microsoft, RealMedia, or AOL) can cause problems when installed improperly on your network, including hidden security holes, inadvertent changes to your system settings, or compatibility issues with other software or hardware that cause your system to stop functioning properly. As a result, it is not uncommon for companies to strictly prohibit the download and installation of internet-distributed software.

Streaming Media

Streaming media files – especially those with full-motion video – leech available bandwidth, leading to a general slow-down of your entire network’s internet connection. In addition, these open connections to the internet can be exploited by hackers, allowing them to penetrate your network security measures. Some streaming media files are even accompanied by pop-up advertisements (more on this below).

Login & Password Caching

Many operating systems, web browsers, email clients, and other applications are able to save login and password information and enter it automatically for you in the future. While this may appear to be a very convenient feature, it can also be very dangerous. If your login and password are automatically entered for you when you load an application or web page, ANYONE using your computer will be able to enjoy the same unfettered access to your programs, documents, and data. This is especially dangerous when using remote access software on your computer (more on this below).

Temporary Internet Files and Browser History

Web pages generally appear on your browser’s screen as complete documents, however the method of displaying web content is more complicated. Each page you view resides on a web server as a single HTML document, with the basic page formatting and text imbedded, as well as references to other files containing graphics, audio, video, and other content. When you visit a web page, your browser downloads this main HTML document into a “Cache” folder or “Temporary Internet Files” folder on your computer, as well as any other content files referenced in this document. While most such files are harmless, dangerous files, such as spyware or viruses, may be among them. In addition, these files can easily take up a large portion of your available hard drive space and can provide a rough log of your web browsing activities. It is therefore advisable to delete these accumulated files regularly. In addition, the exact URL of every web page you visit is stored on your computer as part of your browser history. In addition to providing a complete log of all web activity on your computer, this history may also contain personal information, if any such data was incorporated by a web site into the URL of the page to be displayed (i.e. “<http://www.mybank.com/login/account=123456789/user=johndoe>”). You may therefore

choose to clear your browser history periodically, and browsers generally have a convenient setting to do so automatically.

Cookies

Many web sites use “cookies” in order to store information locally on your computer as you browse. These small files are placed on your computer as you navigate web sites, storing your settings and preferences, and sometimes personal information you provide, including your name, e-mail address, home or work address, or telephone number. When a cookie is saved on your computer, only the web site that created the cookie can read it, and most cookies – though certainly not all – are harmless. For example, some particularly malicious cookies, called “tracking cookies” are specifically designed to gather information about you and your web browsing habits, which is then transmitted over the internet to their owner. This can result in increased spam, pop-ups, and other nuisances, as well as more serious threats to the security of your confidential data, including logins, passwords, and credit card or other account numbers. Most browsers allow you to choose whether to allow cookies to be used. While the safest option is to not allow cookies at all, disabling them may prevent you from viewing certain web sites or taking advantage of customization features (such as local news and weather, stock quotes, etc.).

Remote Access

Remote access applications (such as GoToMyPC and PCAnywhere) and virtual private networks (VPN) have become a key business tool, allowing many professionals to work from outside the office. However, it is important to remember that just as you do, anyone else with your remote access login information can operate your system remotely, as well. Therefore, it is crucial to choose passwords that cannot be easily guessed, to change them regularly, and to keep them strictly confidential. It is equally important to avoid accessing your computer from any public or shared computer, which could be set to remember your username and passwords, or even worse, capture keystrokes or screenshots during your remote session. In addition, it is important to consider the privacy of the computer you are operating remotely. Is it visible or accessible to others in your office while you are operating it remotely? If so, it is advisable to use your remote access software’s screen-blanking, keyboard-locking, and/or mouse-locking capabilities.

Wireless Networking

Wireless technology has revolutionized how information is shared and used over a network, freeing users from the limitations of traditional Ethernet cables. But it is not without its risks. In order to ensure that your data is not read by outside parties, it is crucial that some form of encryption be implemented, such as Wire Equivalent Privacy (WEP), Wireless Application Protocol (WAP), Lightweight Extensible Authentication Protocol (LEAP), or Protected Extensible Authentication Protocol (PEAP). It is also highly recommended that the default login passwords and Service Set Identifiers (SSIDs) be changed. As with any network, wireless networks should be protected from the outside world by an appropriate router or firewall.

Pop-Up Advertisements

Pop-up advertisements have become one of the worst nuisances on the internet. While some web sites use legitimate pop-up windows to display useful information, others are programmed to automatically fill your screen with annoying advertisements, links, and more dangerous threats. Among these threats are viruses and spyware, which can be automatically installed on your system by your browser without your knowledge. There are many pop-up blocking software applications available, and most have a feature to allow pop-up blocking to be temporarily disabled in the event that you are browsing a web site that uses legitimate pop-up windows which you need to view.

- END -