Transferring Data without Secure Protocols?

Don't Leave Any of Your Data Unprotected

You are protecting your VPN access, payroll portal, and payment portal with SSL, right? What about your partner and vendor connections? Have you segregated those connections from your internal network and protected them with SSL?

Whether it is an email to a partner or your customers' credit card numbers, if you are transferring information over an unsecured network (i.e., using HTTP or FTP), that data is in danger of being intercepted.

HTTP and FTP are Vulnerable Protocols

Unprotected data is vulnerable to all sorts of attacks that are not just common, but routine: port stealing, packet "sniffing" (looking for sensitive information), spoofing (pretending to be an authorized user), and bounce attacks (misuse of the PORT command).

Internet crime is a global, multibillion-dollar business.

You Need Encryption to Protect Your Data

Even though SSL is the most common security protocol (HTTPS and FTPS use SSL), some organizations only secure the channels that routinely transfer sensitive data. When you transfer data over HTTP or FTP, your data is "in the clear," meaning if the data is intercepted, it is readable, including usernames and passwords. There is no encryption to protect it. Leaving other channels unsecured is inviting malicious access into your network where villains can worm their way in and wreak havoc on your "secured" networks.

You know that you need to secure your network with SFTP (SSH) or an SSL certificate to help protect the data from malicious abuse. What you might not know is that securing your network isn't as difficult or as expensive to achieve as you think.

It is most certainly not as expensive as what your stolen data would cost your business.

Globalscape's Security Solutions

How do you effectively manage the risk and effects of data breaches, such as the loss of consumer confidence, fines, and other legal penalties? Can you efficiently transfer critical business data, including large files, in a world of social media, mobile workforces, and remote collaboration?

Ultimately, how do you connect business partners, systems, and people, meet security requirements of the government and your business, and still balance the daily needs of your users? Globalscape's solutions deliver complete enterprise security to protect your sensitive data and intellectual property, while allowing your users to remain productive.

Globalscape Solutions:

- Allow users inside an enterprise to send and receive files of any size to and from recipients outside the organization with secure authentication, non-repudiation, and auditing capabilities
- Enforce a comprehensive security strategy by protecting data in motion and at rest
- Support the broadest range of security protocols
- Exceed the highest security levels for data storage and retrieval, authentication, and firewall traversal
- Gauges the risk level of every reported security vulnerability and releases software patches for any affected software, if needed

Contact Globalscape to find out how our security solutions can protect your important business transactions and sensitive data transfers.