Security tips and best practices

Maintaining a vulnerability management program

Experian®, together with our clients, manages extremely sensitive information, requiring the strongest controls to ensure security, confidentiality and integrity. This fact sheet provides guidelines to protect networks and mitigate the possibility of virus infection.

System precautions

- Keep operating systems, firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates. This includes browser software and related plug-ins. Ensure that, where possible, updates are set to automatically occur at least weekly.
- Configure the entire infrastructure, such as firewalls, routers, personal computers and similar components, to industry best security practices, including:
  - Disabling unnecessary services or features
  - Removing or changing default passwords, IDs and sample files/programs
  - Enabling the most secure configuration features to avoid unnecessary risks
  - Creating and enforcing policies on no peer-to-peer computing and on the use of secure USB/attachable devices
- Implement and follow current best security practices for computer antivirus and antispyware scanning, detection and removal:
  - Implement and maintain current, commercially available computer antivirus and antispyware products on computers, systems and networks. These should be continuously enabled for all machines.
  - Antivirus and antispyware applications should be set to automatically download and install definition file updates on a weekly basis. If your company's computers have unfiltered or unblocked access to the Internet, which does not prevent access to some known problematic sites, then it is recommended that updates and scans be completed more frequently than weekly.

- If you are unfamiliar with any of the security measures mentioned above, we recommend that your organization have a certified security professional assess your computing environment to ensure that adequate security precautions are in place and protecting your systems. Note that any PCs used to access Experian data and any devices that are connected to them should be included in this assessment.

Safe computing

- Do not click on links or attachments sent to you in an email unless you know who sent it. These are common delivery methods used by fraud perpetrators to infect computers. If anything about the email is suspicious, a telephone call to verify the identity of the sender is always a good precaution.
- Do not allow computers that access Experian systems to be used to casually surf the Internet. Malware can be installed on a computer by simply visiting an infected Website.

What if?

- If you suspect the presence of actual or potential viruses or spyware, immediately cease accessing Experian systems. Do not use your computer until the problem has been resolved and eliminated. Your information technology department or a certified security professional should be contacted to ensure that all traces of malware have been detected and removed.
- If you believe that one or more of your Experian user IDs have been compromised, immediately contact the Regulatory Compliance Investigations department at 1 800 295 4305.

475 Anton Blvd.
Costa Mesa, CA 92626
1 800 295 4305
www.experian.com

04/11 • **1224/2786** • 5869-CS