New Year's Resolution. . . Resolve to Fight Malware

Make your New Year's resolution to mitigate malware and protect your business and customer data.

For More Information

Visit visa.com/cisp or email cisp@visa.com to learn more about data security tips and resources to help keep your business safe and secure.

Each year, data compromises are increasingly reported in the news and each year different merchant segment are targeted; what remains constant is that cyber criminals continue to develop malware targeting point-of-sales systems. In 2015, Visa observed an increase in the number of data compromises that were tied to existing and new malware families.

To mitigate these attacks, Visa recommends businesses implement the following best practices, including in third party environments where these services are shared or mixed, such as an integrator or restaurant ownership group:

- **Control the Windows Administrator account.** Make privilege escalation difficult.
  - Assign a strong password for all accounts on the Point of Sale (POS) system.
  - Create a unique local Administrator password for each and every POS system.
  - Do not allow users to be local Administrators on a POS system.
  - Change passwords frequently, across the enterprise (at least every 90 days).
  - Do not share passwords.
- **Install application whitelisting on Point of Sale systems.** In addition to anti-virus and anti-malware security, application whitelisting programs are designed to only allow known and trusted executables to be installed and operate. This technology makes it much more difficult to introduce malware onto POS systems.

- **Closely monitor activity on Point of Sale systems.** Be aware of anomalous behavior and investigate all suspicious activity on the POS. Signs may include:
  - New files created in c:\Windows\Installer directory
  - Communication established to external IP addresses over HTTP
  - POS application malfunction (application crashes)
  - Data transfer services (email, FTP) transiting data outside the network
- **Ensure the POS system functions as a single purpose machine.** To reduce the risk of malicious software infections, disallow all applications and services (i.e., Internet browsers, email clients) that are not directly required as part of the POS's core functionality in processing payments.

- **Keep operating system patch levels up to date.** For Windows, this means ensuring Windows Update is functioning and automatically applying monthly security patches. For non-supported operating systems like Windows XP, there should be a plan to migrate to a current operating system as soon as possible.
- **Restrict permissions on Windows file sharing or disable file sharing altogether.** Unless absolutely necessary, Visa recommends disabling file sharing on POS systems. Microsoft has published instructions on how to disable simple file sharing and set permissions on shared folders.
- **Restrict remote access services use.** Unless necessary, disable remote access services, ports and accounts. If remote access services are needed, enable only when needed.
- **Promote security awareness.** Design anti-phishing programs, defense in depth strategies, and promote shared responsibility in security awareness through employee training or educational programs.