D.L. Evans | BANK

Malware & Spyware Software

- What is Malware?
  - Malware, malicious software, is intrusive software that infects your computer, such as viruses, Ransomware, remote access trojans or “worms”.
  - Malware is a computer program that can spread from one computer to another through the internet and other shared devices. It can;
    - Make changes to software and files, restricting your ability to use different applications or prevent access pictures or other personal data stored on the computer or device.
    - Allow remote control of the infected computer or device, allowing the attacker to install more malware, or attack other systems.
    - Provide the means to obtain access to sensitive personal information such as user IDs, passwords, account numbers, and other information. This sensitive information is then later used to commit fraudulent activity at your expense.

- How would my computer become infected with Malware?
  - Malware can be downloaded onto your computer through the internet in the course of browsing questionable as well as legitimate sites. In some cases it will prompt you to install the malware under the guise of protecting your system. In other cases it will install silently in the background.
  - Links within emails, malicious attachments and just opening some specially crafted emails are some other ways your system may become infected.
  - Some web applications used in social media sites can also have malware embedded in them.

- What can I do to avoid downloading Malware?
  - It is important that you have current, fully updated Anti-Virus/Anti-Malware software to thwart most attempts of introducing a malware to your computer.
    - Anti-Virus/Anti-Malware software detects, prevents, and removes most malware from your computer before it is executed on your computer system.
    - It is important to keep your Anti-virus/Anti-Malware software up to date, as new malware is constantly being created to bypass older versions.
  - Never download or open an attachment from an email that has been sent from someone you do not know or from someone you did not expect to receive an attachment from.

- Before opening the attachment from someone you do know, but did not expect an attachment from, it is always best to contact them via phone or text, as their email may have been hacked and someone is using it to send malicious attachments to everyone in their contact list.
- Only install web applications from trusted sources and be careful to review the permissions granted to the applications.

Important Information

D.L. Evans Bank will not request personal or sensitive information (full Social Security Number, passwords, full Debit/Credit Card Number, or PINs) when contacting you. However, D.L.Evans Bank or our authorized Fraud Department may contact you regarding suspicious transactions on your account and request information to verify your identity. If you are suspicious of these automated phone calls, you are welcome to call us to ensure the phone call was indeed valid. We can be reached at 208-678-2552 or 1-866-661-5463, Monday through Friday from 8:00 am – 5:00 pm.