visual-eyes
Simplify Your Life!

Unit 286 -4819C 48th Avenue
Red Deer, AB, T4N 3T2
Tel: (403) 314-1322
Fax: (403) 314-1320
Email: support@visual-eyes.ca

Avoiding Online Security Scams

In today's age of technology, it is important to be increasingly aware of scams regarding our computers, and in turn, patient information. A common scam found online today allows a malicious user access to your system. The user typically gains access via cold calls and fake warning messages that connect you to a live person trying to access to your system. It is imperative that all staff are aware that companies such as Microsoft will never prompt you to contact them with an ad, or call asking for access to your computer unless you have initiated the contact first.

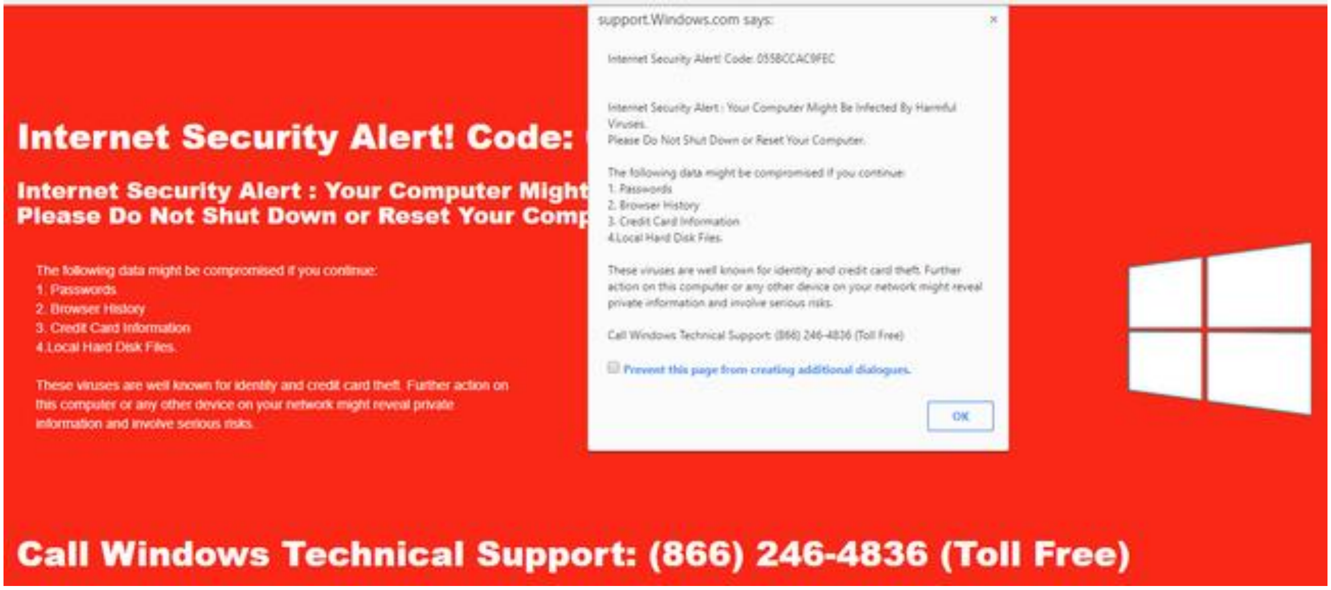
If you suspect a system in your office has been made vulnerable to a scammer, please contact your local IT immediately to investigate and clean up your system. Depending on privacy acts in your province you may also be required to report any unauthorized users accessing a Visual-Eyes workstation. Below are a few ways we can recognize and avoid harmful scams.

Calls:

Calls will often come in claiming to be from Microsoft Support. They will attempt to convince you that there is an issue with updates, or your installation of Microsoft Office. They will often ask you to allow them into your system via remote software that they will instruct you to download. Microsoft will never contact you unless you have initiated the contact first. Any call coming from someone claiming to be from Microsoft support should be immediately disconnected.

Fake Warnings:

Some Ads online will attempt to load large error messages onto your screen, asking you to contact Microsoft Support, and provide you with a phone number to call. Like the cold calls, Microsoft will never prompt you to contact them to provide remote access. If you receive any error messages on your system that are causing disruption to your normal computer use, always contact your local IT contractor first. No third party asking you to call them unprompted has your best interests in mind. An example of scam error message is on the following page.



Internet Security Alert! Code:

Internet Security Alert : Your Computer Might
Please Do Not Shut Down or Reset Your Comp

The following data might be compromised if you continue:
1. Passwords
2. Browser History
3. Credit Card Information
4.Local Hard Disk Files.

These viruses are well known for identity and credit card theft. Further action on this computer or any other device on your network might reveal private information and involve serious risks.

support.Windows.com says:

Internet Security Alert! Code: 055BCCAC9FEC

Internet Security Alert : Your Computer Might Be Infected By Harmful Viruses.
Please Do Not Shut Down or Reset Your Computer.

The following data might be compromised if you continue:
1. Passwords
2. Browser History
3. Credit Card Information
4.Local Hard Disk Files.

These viruses are well known for identity and credit card theft. Further action on this computer or any other device on your network might reveal private information and involve serious risks.

Call Windows Technical Support: (866) 246-4836 (Toll Free)

☐ Prevent this page from creating additional dialogues.

Call Windows Technical Support: (866) 246-4836 (Toll Free)

Potential Issues:

Scammers will often load various viruses, or cryptocurrency miners which may not cause any visible harmful effects. However, once these users have accessed your system they have the ability to upload local files to their systems to use for identity theft, or resale of medical data. They may also run miners on your system which can cause system slowdowns or crashes. If you suspect a system in your office has been made vulnerable to one of these events, please contact your local IT immediately to investigate and clean up your system.

Following Protocol:

If your Visual-Eyes workstations are accessed by unauthorized users, you may need to report the intrusion per the various healthcare privacy acts in your province. Please review your province’s Privacy Laws regarding Medical Data to determine the appropriate actions if this kind of event transpires.