BBB NEWS
Better Business Bureau
Serving Minnesota and North Dakota
220 S. River Ridge Circle
Burnsville, MN 55337
651-699-1111
651-699-7665 (Fax)

FOR IMMEDIATE RELEASE

Bogus Computer Alerts Play on Fear, Embarrassment

Scammers claim computers contain adult content

Burnsville, Minnesota – August 9, 2018 – Better Business Bureau® of Minnesota and North Dakota (BBB) is warning consumers about a newer scam that's affected other parts of the country and seems to have moved into our area – a fake "pop-up" alert scam which tells computer users that adult content has been detected on their computers. People are then urged to call an 877 number before closing the page or their "computer access will be disabled to prevent further damage to our network." The alert also says, "Financial data, Facebook Logins and credit card details are being stolen." However, these alerts are not legitimate and unknown entities behind them are fraudulent.

"This is yet another scam that operates on fear and uncertainty," said Susan Adams Loyd, President and CEO of Better Business Bureau of Minnesota and North Dakota. "Fraudsters are counting on consumers being willing to make a payment to avoid potential embarrassment. We're telling people not to panic and not to play into the hands of scammers, as they are very likely bluffing."

Though these "alerts" look scary, they only become dangerous when people call the phone numbers that accompany these messages. BBB urges people to simply close the page – or their browser – and the suspect alerts should go away. BBB recently received one of these alerts and called the support number listed – an 877 number. The person who answered claimed they were working with Microsoft (a claim that fraudsters often make) and offered to run a free scan of the affected machine. At that time, BBB ended the call. Allowing anyone remote access to your computer puts your device and sensitive personal and financial information at great risk.

The malware which triggers these bogus alerts is often acquired by innocuous browsing of mainstream websites. A good way to avoid such alerts is to have anti-virus and anti-spyware protection on your computer. It's also best to avoid any suspicious or compromised websites. But it's important to know that anyone with a computer – regardless of their browsing habits – can receive such alerts.

"The alert that was brought to our attention claimed the user had just five minutes to contact the support number provided to prevent their computer from being

disabled or from any information loss," added Adams Loyd. "Obviously, that's very scary. People need to stay calm and recognize these alerts for what they are."

BBB of Denver issued an alert on a similar scam late last year, wherein people received emails from self-proclaimed hackers who attempted to blackmail victims through a series of emails sent to victims' work email addresses. The first emails contained adult content and links to dating websites, soon followed by a message demanding payment – in Bitcoin – from those who had clicked on the links. In the subsequent message, the scammers also claimed to have hacked the victims' webcams and threatened to share captured video and screenshots from adult websites to people in the users' email and social media contact lists.

In those cases, experts said such threats were likely empty ones. Though it is possible for scammers to hack webcams, BBB advises people not to make any payments to people claiming they have done so and to report any threats to local authorities, as blackmail is a crime. BBB also advises employees not to engage with any suspect emails they receive and to avoid clicking on links or attachments in such emails. It's also a good idea to cover your webcam when not using them for a Skype call or video chat.

More recently, the Detroit Free Press reports that scammers are now contacting consumers via email and threatening to share their online browsing histories unless a payment is made. What's more, scammers in these cases have somehow gained access to old but legitimate usernames and passwords that victims have used at one time.

BBB's advice to the public remains the same: don't panic. Keep in mind that a lot of personal information – including old usernames and passwords in some cases - has been made available through various high-profile data breaches in recent years. Successful phishing attacks, wherein scammers gather sensitive personal data through impersonation schemes conducted via email, are another source of information fraudsters use to their advantage.

If you're concerned about an alert you've received on your computer, contact BBB (bbb.org) to report your experience and get expert advice. Don't call the phone numbers that appear within these alerts, as they're part of the scheme. When in doubt, exit out of the page you're on, close your browser or simply shut down your computer. If the alerts won't go away, you may need to contact a technical expert.

Media Contact: Dan Hendrickson, Communications Manager
651-695-2463 / dan.hendrickson@thefirstbbb.org

The mission of Better Business Bureau is to be the leader in building marketplace trust by promoting, through self-regulation, the highest standards of business ethics and conduct, and to instill confidence in responsible businesses through programs of education and action that inform, assist and protect the public. We are open 8 a.m. to 5 p.m. Monday through Friday. Contact BBB at bbb.org or 651-699-1111, toll-free at 1-800-646-6222.