CTSI
TECHNICAL UPDATE
Volume 28 Number 40 | October 1, 2024

CYBERSECURITY INSIGHTS: FAKE LOGIN PAGES AND MALWARE OFFICE SUITE

In today's digital age, cybersecurity is a critical concern for counties of all sizes. As cyber threats become increasingly sophisticated, counties must stay vigilant and proactive in protecting their sensitive data. CTSI will stay informed of evolving threats and provide quarterly cybersecurity updates on the latest concerns, best practices, and security protocols. This knowledge can significantly reduce the risk of a successful cyber attack and promote a security-first culture.

FAKE LOGIN PAGES

A popular method to steal your credentials is using fake login pages to capture your login details. These attacks usually start with a phishing email that directs you to use a link in the email to "log in to your account." The emails are generally authentic-looking and present a seemingly ordinary request. If you click this link, you're brought to a login page that looks almost identical to the one you're used to but is a fake page. Once you've entered your email and password on the fake page, you may be redirected to the actual website–leaving you unaware that your login credentials were stolen. Once the hackers have your login information, they can even sell it for payment.

HOW TO SPOT A FAKE PAGE

As the first line of defense, always navigate to your account's login page by typing the web address in your browser or using a bookmark that you've saved–rather than clicking through links in an email. Also, be aware of the following tips to help you identify fake web pages:

- Check the address bar and domain name. To avoid fraudulent sites, ensure the website starts with "https://" and the domain is correctly spelled.
- Watch for poor grammar and spelling. Excessive spelling, punctuation, or grammar mistakes can be a sign of an untrustworthy site.
- Be cautious of deals that seem too good to be true. If an offer looks unusually generous, it's likely a red flag. Always verify before purchasing.

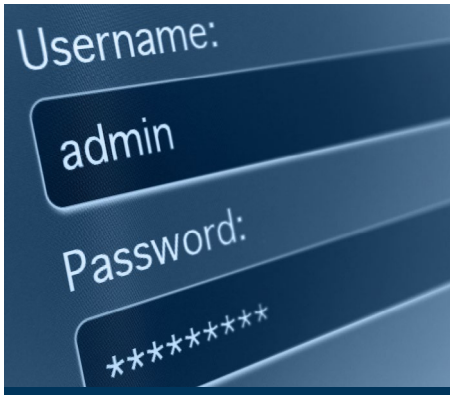
MALWARE OFFICE SUITE

"You get what you pay for," and this timely scam is no exception. Cybercriminals are distributing a "free" pirated version of Microsoft Office across torrenting websites. The catch is that it's malware. The malware can begin harvesting your personal data if you download and install it.

The installation process appears legitimate if you download the malicious Microsoft Office file. The installer looks professional and allows you to select the Microsoft Office version you want to install. However, if you run the file, malware will install on your computer. The malware is designed to avoid detection from most antivirus systems. Even if your antivirus software scans and removes it, this particular malware can re-install itself afterward. This "free" version of Microsoft may cost you something - your data!

Follow these tips to avoid falling victim to a malware scam:

- Never download software from unofficial sources. A pirated software version isn't an official release and may contain malware.
- If something is too good to be true, it probably is. You usually pay for Microsoft Office; a free version isn't likely legitimate.
- Follow your organization's instructions regarding antivirus software and data backups. Updated software and data backups can help protect your machine from malware infections.



WHAT THIS MEANS FOR COUNTIES

Regular cybersecurity updates are vital to an effective security strategy. They help keep counties informed, vigilant, and prepared to respond to threats. CTSI recommends counties implement these essential cybersecurity controls to help manage their cyber exposures. This will safeguard and reduce digital vulnerabilities at the county level and assist in obtaining coverage with higher limits and lower premiums for CAPP. For more information, contact CTSI at (303) 861-0507.

County Technical Services, Inc.
Technical Updates are available online at ctsi.org
800 Grant St., Suite 400, Denver, CO 80203
(303) 861-0507 | Fax: (303) 861-2832