Watch out for FAKE domains and email addresses

In our digital era, we get A LOT of emails, with that comes risk. One significant risk is fake domains, designed to mimic familiar email addresses and websites. These deceptive domains, also known as domain spoofing or typosquatting, are associated with phishing attacks, malware distribution, financial losses, and reputational damage. In this article, we'll explore the importance of being vigilant about spotting fake domains and ways to protect ourselves online.

Volume 23, Issue 8
August 2023

How do you recognize domain spoofing?

Domain spoofing is when cybercriminals create deceitful websites that closely resemble legitimate ones. They use slight misspellings, homoglyphs, or different top-level domains to deceive users. For example, "amaz0n.com" instead of "amazon.com."

Examples of the techniques used by cybercriminals:

- **Typosquatting:** Registering domains with common typing errors related to known websites.

  Legitimate domain: www.WestMichiganConstruction.com

  Typosquatting domain: www.WestMichiganConstructlon.com

  Legitimate domain: www.instagram.com

  Typosquatting domain: www.instagrarn.com

- **Homoglyph Attacks:** Utilizing characters from different character sets that look similar to those in the original domain and are much harder to spot.

  Legitimate domain: www.amazon.com

  Homoglyph attack domain: www.amazon.com

- **Subdomain Spoofing:** Creating subdomains resembling legitimate ones to deceive users.

  Legitimate subdomain: login.microsoft.com

  Spoofed subdomain: login-microsoft.com

So, what can you do the help keep yourself safe?

- **Scrutinize the Sender's Email Address:** Check the sender's email address carefully. Look for unusual characters or domain names that differ from the expected sender.

- **Verify the Domain:** Hover your mouse over any links or buttons in the email without clicking. This will reveal the actual URL the link points to. Ensure the domain matches the legitimate one associated with the organization. Be cautious if the domain appears suspicious or unrelated.

- **Enable Email Authentication:** Ensure your email provider has enabled authentication mechanisms like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) to help detect and block spoofed emails.

- **Report Suspicious Emails:** If you receive a suspicious email, report it to your email provider or the organization it claims to be from. This helps them take appropriate measures to protect their users and prevent further spoofing attempts. If emails are going to your clients with a spoofed domain that looks like **YOUR** company name, let your clients know and help them learn what to watch for.

As cyber threats grow, it's crucial to remain vigilant against fake domains. By being cautious online and following these simple steps, we can protect ourselves from phishing attempts, malware, and financial losses.

At Aeros we believe in keeping you informed to try to keep you safe. Please, let us know if you have any questions or concerns.

Is your hard drive encrypted?

Knowing whether or not and by what means your hard drive is encrypted is very important these days. Some new computers now come with the Microsoft BitLocker enabled from the factory. Also, companies that deal with medical information and records, financial records, or store personal protected information about their employees on their work systems are required by regulations to have that data encrypted to a specific minimum level.

What do you need to know about encrypting your drive?

First, it is a relatively easy process to encrypt and decrypt your drive(s) for use. One of the key things you need to keep in mind is that you **MUST** store the decryption recovery keys in a safe location. If you don't record and store your key properly or if you lose it, you can potentially lose access to **ALL OF YOUR DATA.**

Second, you should know which systems are encrypted and monitor them if encryption is required or you feel that it is something important that you want to maintain. This means regularly checking each system to ensure that the drive continues to be encrypted and then doublechecking your recovery key.

We have witnessed way too many people try to protect their data and end up losing it all because although they had the data encrypted, they didn't back it up, and they didn't take care of their recovery key. When their computer died, the data was encrypted with no way of decrypting or recovering it.

So, what do you need to do?

If monitoring and storage of your drive encryption feels like too daunting of a task, but you want or need to do it, we have some great news!

We have started a new service to help companies with their drive encryption needs. Starting at only $30 a month per company, we will enable drive encryption on all installed/internal drives on the workstation/server, document and store the recovery keys in our own encrypted storage, monitor the systems to ensure that the system remains encrypted and notify you if someone decrypts a drive.

If you are interested in the new service or if you have any questions about drive encryption, please don't hesitate to reach out to us.

Aeros IT Group

6261 Lake Michigan Drive
Allendale, MI 49401

Phone: 616-997-8324
Email: support@aerosgroup.com

Building Relationships in West Michigan since 1976!

Aeros

A DIFFERENT WAY TO I.T.