Look-alike Websites

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity, safety, and respect

More and more people use the Internet to access government services and for personal business transactions. People can change mail delivery, renew license tabs, sign up for health insurance, and order credit reports online. But with this increased accessibility comes added risk: look-alike websites that charge unnecessary fees, provide inaccurate information, or do not deliver any services at all. It can happen like this:

What to Look For

As a first-time business owner, **"Emily"** searched the Internet to learn more about receiving a business tax identification number. She filled out a form on a "*.com*" website and paid $125 to what she thought was the Minnesota Department of Revenue, but she never received the documents she ordered. When she called the Department of Revenue, Emily learned that its website was *revenue.state.mn.us* and that a business tax identification number is free.

When using the Internet, it is important to ensure you are dealing with the correct entity. Legitimate websites are upfront about their identity and services. Look for clues like the extension (ex: *.com*, *.org*, *.gov*, *.biz*, *.net*) of the web address. While there are few hard and fast rules dictating which types of entities can use each extension, it is one potential indication of a website's security. For instance, look for the *.gov* extension on government websites.

→ **To find reliable links to all Minnesota State agencies, boards, and commissions, visit the portal at *mn.gov/portal/government/state/agencies-boards-commissions*.**

Before applying for a car loan, **"Ryan"** went online to look at his credit report. A month later, he found a charge on his credit card for a credit monitoring service. The website Ryan used offered a free credit check, but the fine print included a "trial" credit monitoring service. Ryan didn't know that *annualcreditreport.com* was the only place to find his free report.

Similarly, pay close attention to icons—like the padlock—that appear in your URL bar when you are visiting an encrypted, or secure, website. Depending on the Internet browser you use, the URL bar may be shaded a different color when a website is secured. Also, look for "*https://*" (the "s" is for secure) before the web address, because this indicates that the website and Internet connection are secure. In general, "*http://*" websites are vulnerable to attack.

→ **Never provide personal or financial information to insecure or unencrypted websites because fraudsters can "eavesdrop" on this information.**

"Michael" recently moved across town and needed to update the address on his driver's license. He entered "driver's license address change Minnesota" into a search engine and clicked on the first link that appeared. At first glance, the website looked very similar to the State of Minnesota Department of Vehicle Services website, *dps.mn.gov/divisions/dvs*. The website's banner also had the same graphics and color scheme as the official State website. He filled out an application and paid a $15 fee before realizing he was on the wrong website.

Typing a word or phrase into a search engine will typically bring up thousands of hits, but search engines often place advertisements and sponsored websites (i.e. websites that pay to be the first result of a search) more prominently than legitimate hits. Advertisements can be tricky to spot because they are typically listed on a lightly shaded background or sidebar, where many people mistake them for legitimate websites.

→ **Know that the website you are looking for may not be the first one listed.**

"Christina" wanted to re-direct her mail while she was away at college. She ordered an address change from a website that had a logo similar to that of the United States Post Office—only instead of a blue eagle, the website had a blue bear. Christina missed the nuance and paid $40 for the purported service. Her mail was not forwarded and when Christina called her local Post Office, the representative told her that changing an address online costs $1.

Websites often place a seal from organizations such as the Better Business Bureau, VeriSign, or McAfee to promote the website's reputation or security. On legitimate websites, these seals should be links to those organizations, not just photos.

→ **Click on branded logos and "seals of approval" to be sure you know who you are dealing with.**

Tips

- Never click on links in emails or pop-up advertisements. Scam artists use familiar logos and similar-sounding web domains to lure Internet users to fraudulent websites.
- Use a reliable source, like a phone book or the government portal listed above, to double check the contact information for state agencies.
- Report look-alike websites to the agency or organization that is being imitated.