SCAMS REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING FEBRUARY 14, 2022
Submitted by Arnold H. Shifrin

How To Spot A Fraudulent Website

Most of the almost two billion websites on the internet are legitimate. Some sites, however, are phony and are run by scammers trying to steal personal information and money from their victims. Here are several ways to help spot a fraudulent site.

1. **Check the web address (URL name):** Scammers create websites with names that are similar to those of their legitimate counterparts. The goal is to trick victims into believing they are dealing with the actual site. The difference in the names of the real and phony sites can be very subtle. For example, you may think you're visiting *amazon.com*, but you're actually visiting *amazom.com*. Or, you may think you're visiting *microsoft.com,* but you're actually visiting *rnicrosoft.com.* (Notice the spelling of the URL names "a m a z o m" and "r n I c r o s o f t.") Once you've accessed a fraudulent site, you are vulnerable to identity theft and the loss of money from your accounts.
2. **Look for the padlock icon and "https" in the address bar:** These signify the information transmitted between the user and the website is encrypted and the site is secure. Secure sites are issued a certificate to confirm that users are protected. You can verify that a certificate is valid and view details of the certificate on a PC by following these steps: a) double-click on the padlock in the address bar, b) click on "Connection is secure," and c) click on "Certificate is valid."

   Some sites that are not secure contain a padlock icon in the address bar with a strike through it or a message stating "Not secure." Do not provide personal or financial information on sites that are not secure.
3. **Verify the website's privacy and return policies:** Many fraudulent websites do not contain customer return and privacy policies. If the policies are included, they are often brief and poorly written. Before completing an online transaction, be sure to review the site's policies to make sure they meet with your approval. Consider, for example, if you can return or exchange an item without paying a penalty. Avoid conducting business on sites without acceptable policies.
4. **Check for spelling and grammatical errors:** If a website contains spelling and grammatical errors, it may be operated by scammers in another country with a poor command of the English language. Legitimate sites are designed by trained professionals and are usually error-free. Avoid entering personal or financial information on sites with these errors.

Steps to take if you're the victim of an online scam

- If you made a purchase on a fraudulent site with a credit or debit card, report it to the issuing bank. They will freeze your account and give you a new card.
- If you provided credit card or personal information on a fraudulent site, report it to one of the three credit bureaus: 1) Experian (*experian.com);* 2) Equifax (*equifax.com);* or 3) TransUnion (*transunion.com*). The credit bureau to whom you report the incident will notify the other two. All three bureaus will freeze your account to prevent fraudsters from taking out loans or opening new accounts in your name.
- File a report with the Internet Crime Complaint Center (IC3) at *ic3.gov.* The IC3 refers complaints of suspected internet criminal activity to the FBI for investigation.
- File a report with your local police department.

[Sources: Home Bank of California, How-To Geek]