SCAM REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING JANUARY 8, 2024
Prepared by Arnold H. Shifrin

Fake Websites

Background: Scammers create fake websites that closely resemble legitimate ones to trick potential victims into visiting them. Once someone accesses a fake site, scammers can steal their personal and financial information and infect their device with malicious software.

Components of a website address

- **https://www.example.com** is the format of a typical website address (the address is also known as the URL which stands for Uniform Resource Locator)
- **https is the protocol** (stands for Hypertext Transfer Protocol Secure)
- **www is the subdomain** (stands for World Wide Web); this is no longer needed to access a website
- **example.com is the domain name** (sometimes referred to as the hostname)
- **.com is the domain extension**

Examples of legitimate domains

- google.com
- walmart.com
- amazon.com
- fbi.gov
- irs.gov
- ftc.gov
- redcross.org
- cancer.org
- illinois.edu
- caltech.edu

Examples of scammers' fake domain names

- gooogle.com (there are three "o's" instead of two)
- arnazon.com (the 2nd and 3rd letters are "r" and "n", respectively, instead of an "m")
- bankoffamerica.com (the word "of" has an extra "f")
- waImart.com (the 3rd letter is a capital "i" instead of a lowercase "L")
- delivery.ips.com (the word "delivery" was added to hide the fact that "ups" is spelled "ips")
- netflix-support.net (the correct domain extension for Netflix is ".com" not ".net")

How to identify fake websites

- Closely examine a website's domain name before opening attachments or clicking on links.
- Look for spelling and grammar errors and other misuses of the English language.
- Be cautious if a website uses "aggressive" language to get you to act immediately or out of fear.
- Examine how a site is designed. Be sure the graphics and visual quality are what you would expect from a legitimate site.
- Look for "Contact Us" and "About Us" pages. Legitimate websites do not hesitate to provide this information to their site visitors. If this information is not provided, it may indicate the website is fake.
- Pay attention to shopping websites with addresses ending in ".net" or ".org" as these are not common domain extensions for shopping sites.
- To reach a legitimate website, be sure the address you enter in your browser's address bar is one you know is correct. Do not use an address that was given to you by someone else.

If you were the victim of a fake website scam, take the following steps

- Notify your credit card issuer. They will close your account and issue you a new credit card.
- Change the passwords for all your online financial accounts. Enable 2FA for added security if offered.
- Freeze your credit with the three major credit bureaus (TransUnion, Equifax, Experian).
- Monitor your financial accounts daily for unauthorized activity. Do not wait for monthly or quarterly statements
- Report the incident to the following agencies:
  - Internet Crime Complaint Center (*www.ic3.gov*)
  - Federal Trade Commission (*reportfraud.ftc.gov*)
  - Your website browser (e.g., Google Chrome, Microsoft Edge, Apple Safari, Mozilla Firefox)
  - The legitimate business entity with whom you thought you were dealing (e.g., amazon.com, ebay.com, walmart.com)
  - Illinois Attorney General Senior Citizens Consumer Fraud Hotline (1-800-243-5377)
  - Your local law enforcement agency.

[Sources: Aura Identity Protection, Kaspersky Co.]