** Cuyahoga Community College Top 10 Information Security Tips**

|  |  |
| --- | --- |
|  | 1. **Hover to discover.** “Hover” the mouse cursor over a link to see where it leads before you click. If it does not lead to where you expect or looks unusual, ask or do not click.
 |
|  | 1. **Be cautious of attachments and links** in email – even from people you know.  The sending address might be spoofed or the account could have be compromised.  If you think you received something odd from someone you know, call them before acting.
 |
|  | 1. Click the **PhishAlert** button to report phishing messages. This sends them to the information security team.
 |
|  | 1. Before typing your username and password into a site, **check the URL bar** to ensure it is a College website (\*.tri-c.edu) and that it has the padlock symbol to show the connection is encrypted.
 |
|  | 1. **Report unusual activity** by emailing information.security@tri-c.edu, emailing or calling the helpdesk, or call 216-987-4171 for David Mastny, Manager of Information Security.
 |
|  | 1. **Take the on-demand Security Awareness training modules** every year to refresh and view updated content. These are available in the TEC learn system which you can access through “My Tri-C Space” in the “Employee” tab.
 |
|  | 1. **Choose a strong password**. Avoid dictionary words. Hackers know how people choose passwords. If uppercase, lowercase, numbers, and symbols are required, most people will start off with a word with the first letter capitalized, the rest lowercase followed by a number and then a symbol. The symbol is more likely to be an exclamation point than other characters. Choose a password that does not follow this convention. Do not use any part of your username (forward or backward), any word related to Tri-C, sport teams, seasons, year, keyboard patterns.
 |
|  | 1. **Handle sensitive data such as SSN or credit cards appropriately**. Do not send this data over email and do not store on computer hard drives or portable media. Store only in a College-approved location where access is restricted to only those that need it.
 |
|  | 1. **Be on the lookout for suspicious calls requesting info or access to your computer**. These kinds of calls are becoming more common, including those impersonating tech support. Also, you cannot trust the caller is really calling from the number reported by CallerID because it can be spoofed. Report to the helpdesk or your information security team as in tip #5 above.
 |
|  | 1. **Do not reuse passwords – use a different password for every important account.**  Websites get hacked and their passwords get leaked. Hackers know that people reuse passwords and have automated tools to test to see where else a leaked password is used. If you use the same password in more than one place, a breach of one site can lead to a breach of your accounts at other sites.
 |