DigiKnow
CYBER SECURITY DEPENDS ON YOU

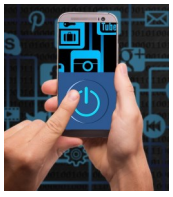
SECURITY CONCERNS AT WORK AND AT HOME

September's here and at DTI we're preparing for the Secure Delaware Conference and Cyber Security Awareness month in October. In the background, we're adding resources to dramatically improve the State's Security Operations Center. Be watching for cyber safety awareness sessions throughout state government and in the community, too.

— *Solomon Adote,* Chief Security Officer

Browser Extensions Selling Your Data?

The Washington Post's July 2019 Consumer Tech column reported that as many as four million people have web browser extensions that sell their users' every click. All sorts of personal and corporate data were leaked via Chrome and Firefox, an independent researcher has discovered. Once informed, Google and Mozilla shut these leaks immediately, but it's probably only part of larger problem.



Browser extensions, also known as plug-ins or add-ons, are used by about half of all desktop website surfers. They enhance browsing experiences, doing everything from finding coupons to saving passwords. People install them believing that if they're downloaded from a Firefox or Chrome store they are safe and secure. This is not always the case.

Academic researchers say thousands of extensions profit by gathering browsing data — many with loose or downright deceptive data practices — lurking in the online stores of Google and even the more privacy-friendly Mozilla.

How to stay safe? Use as few browser extensions as possible. Uninstall extensions you rarely use. Check the permissions, if possible, required by the extension before installing it. Many require access to everything (e.g., camera, microphone, contacts). Consider the value of the extension versus the potential that your data could be exposed and sold. Finally, if you are interested in an extension, do some online research before installing.

Phishing for Ransomware? Cyber Thieves Are!

***"The main purpose of most phishing emails today is to deliver, directly or indirectly, some form of ransomware."* —** Deloitte.com

The best defense against phishing ransomware attacks is an informed workforce. By getting ready for these phishing attacks, users can be empowered to act as both "human sensors" for spotting phishing attacks and partners in thwarting threats from gaining a foothold in the organization.

Listed below are highly effective phishing emails that end-users need to be vigilant about:

- Corporate emails resembling official corporate communication (e.g., benefit enrollment messages, full mailbox notices, etc.);
- Commercial, business-related emails that are not organization-specific (e.g., wire transfer requests, insurance notifications, shipping confirmations, etc.);
- Consumer emails the general public gets on a daily basis (e.g., social networking notifications, gift and greeting cards, etc.);
- Technical emails such as error reports and bounced email notices.

Organizations should follow a variety of best practices that organizations to minimize their exposure to phishing and ransomware. These include implementing a strong security awareness program to educate users to make better decisions about the content they receive through email, on what they view or click in social media, and how they use their web browsers. It is essential to sufficiently invest in employee training so that the "human firewall" can provide an adequate first line of defense against increasingly sophisticated phishing and ransomware.

Questions, comments or topic suggestions? Email us at eSecurity@delaware.gov

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or want to print a PDF copy, go to https://digiknow.dti.delaware.gov.