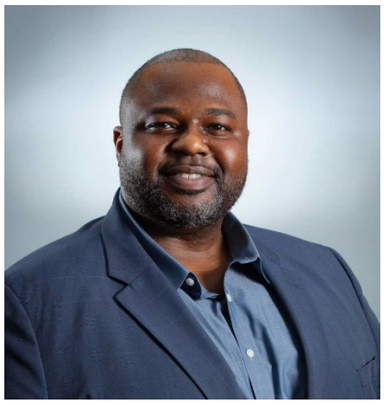
# DigiKnow

CYBER SECURITY DEPENDS ON YOU

## BROWSERS - GATEWAYS TO THE INTERNET

December 2022 | Issue 2022:10



### THE EVER-CHANGING CYBERSECURITY LANDSCAPE

As your Chief Security Officer, I am committed to evolving to the changing cybersecurity adversary. Today's bad actors are more sophisticated than ever before. It is imperative to keep an eye on the tactics, techniques, and procedures attackers are using.

One example is a new breed of phishing emails. The content and the coding change dynamically, making it harder for our controls to detect. Unlike a generic phishing attempt, this new approach is capable of changing its content based on the targeted organization's email domain.

This allows the malicious actor to widely distribute phishing emails that appear to be a lot more credible in a much shorter timespan allowing improved quality and quantity and therefore increasing their success rates.

We are focusing our efforts to meet challenges such as these in a variety of ways. One of our first steps was the shift to using multi-factor -authentication for logins.

Education and training also are important components in combatting cybersecurity adversaries. The checklist below is a great resource to share with family and friends.

### SURVIVING AN EMAIL HACK

If you suspect someone has hacked into your personal email, do this IMMEDIATELY:

1. Don't panic

## BROWSER SAFETY

Browsers such as Google Chrome, Microsoft Edge, Apple Safari, or Mozilla Firefox are the way most people interact with the Internet. We use them for checking the news, email, shopping online, watching videos, and playing games. As a result, browsers are also a target for cyber criminals and attacks step up during the holiday shopping season. In this article, you'll find ways to secure your browser and protect your information.

**Updating**: Always use the latest version of your browser. Updated browsers have the latest security patches and are much more secure. Updating today is as easy as simply enabling automatic updates on your system. After an update, check for additional new security features.

**Warnings**: Today's browsers can often recognize certain malicious websites designed to cause you harm. If your browser warns you that the website you are about to visit is dangerous, close your browser tab and find what you need on a different website.

**Syncing**: Never sync your work browser with your personal browser or any personal accounts. Syncing is when you enable browsers on different devices to talk to each other and share your browsing information, such as your browsing history, bookmarks, and saved content.

**Passwords**: Many browsers support the option of saving your passwords to different sites. Instead of storing your passwords in your browser, it is recommended that you use a dedicated password manager. Password managers are a separate security application that have far more security features and functionality.

**Plug-ins**: Plug-ins or extensions are small pieces of software added to browsers that can provide additional functionality. However, each new plug-in you install can create more vulnerabilities. For your work computer, only add plug-ins that are authorized and approved, and just like your browser, keep them updated. Remove plug-ins that you no longer need or use.

**Privacy Mode**: Most browsers offer a privacy option (also referred to as "incognito mode"). This means when you open a browser tab in privacy mode, you limit what information is collected about you. For example, your browser does not collect cookies, does not track browsing history, and will not store nor distribute sensitive information about you.

**Live Chat**: Some websites now offer a live chat feature where you can ask questions. Only engage in these online

2. Log into your email
3. Force logout of all active sessions
4. Change your password
5. Enable multi-factor authentication
6. Delete any unknown "forwarding" addresses and rules
7. Delete any unknown mail filters and rules
8. Reset the passwords for all accounts tied to that email address
9. Set up credit monitoring & bank alerts
10. Tell your family, friends, and frequent contacts to be on the lookout for scams and fraud coming from "you"
11. Submit a report to the FBI's Internet Crime Complaint Center (IC3)

Wishing you a happy and cybersafe holiday season.

Solomon Adote
Chief Security Officer

chats with known, trusted websites. In addition, limit the information you share during a live chat session, as you have no idea who is collecting your information, what they are doing with it, and if they are selling it or sharing it.

**Beware of Remote Control**: Fraudulent websites will attempt to hack your computer by posting a fake security pop-up warning to your browser that your computer is infected and pressuring you for an online chat session to fix your computer. They will then urgently request that you allow them to install a remote agent to allow them to fix your computer. They are attempting to trick you into installing malicious software so they can steal your passwords and your data, and track all of your online activity.

**Log Off**: When you are finished visiting a website, be sure to log off to remove sensitive login and password information before closing the browser.

Information Provided by the SANS Institute

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Information & Technology 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/news/index.shtml?dc=newsletters