Five ways to be more cyber-secure

A quick reference guide for users at Indiana University

**Sign up for Two-Step Login**
Protect your account by setting up two-step logins. Every time you log in to the Central Authentication System (CAS), you'll receive a smartphone notification, a text, or a voice call to confirm you are you. You can also use a Duo token if you already have one. Two-step logins can prevent hackers from accessing IU data, even if your passphrase has been compromised. Search One.IU for “Two Step” to get started.

**Learn about phishing**
Phishing scams are typically fraudulent email messages that appear to come from legitimate senders. UITS provides general phishing education in its Knowledge Base – for an overview and links to helpful material, visit kb.iu.edu/d/arsf. The National Cybersecurity Alliance also provides information on a variety of topics, including phishing, at https://staysafeonline.org.

**Closely inspect sites that ask for credentials**
This summer, CAS got a new look. The new site has username and password fields that change size and color when you click them, making them harder for hackers to spoof. Also look for the secure lock next to the URL every time you login.

**Sign up for foreign log alerts**
You can choose to receive an email notification if someone from outside the United States logs in with your account. To receive alerts, go to logins.iu.edu and choose “Send emails for non-US logins.” If you see a login that you weren’t expecting, contact UIPO immediately by email: IT-Incident@iu.edu

**Look for and verify digital signatures**
Digitally signing messages signals to email recipients that a hacker has not compromised the sender’s account. Be sure to look for and verify digital signatures on messages from Workflow and other official notifications as an added layer of security.