@DeldigiKNOW

DigiKnow
CYBER SECURITY DEPENDS ON YOU

May 2019

Picture Perfect - Be Safe On Instagram

Ahh, the month of May - time for flowers, proms, graduations and of course, Mom. Take a moment to learn how to stay safe on Instagram and then catch all these special moments digitally.

Instagram 101

Always Think Before You Post!

The number one thing to remember is that Instagram is a social network. This means that you should ***only post photos and videos*** you believe are appropriate for the general ***public***. Don't forget that anything you post to the Internet may be viewed by people you know as well as people you don't know.

Use Instagram's Privacy Options

Set your account to **Private**. This requires people to submit a request to follow you before they can see your posts. Approve only those followers you know: you have much more control over who can see your posts. Use "Instagram Direct" to share posts directly with people (even if they aren't your followers). Sharing directly and only with people ***you*** choose keeps what you post from showing up on any of your profiles or in any tag searches.

Be a Decent Digital Citizen

You may see a photo, caption, or comment that causes you anger or distress. It's tempting to comment, express your displeasure, or start an argument, but avoid the temptation to flame. Make the Internet a better place by making positive comments. ***Keep Instagram a positive place: report threatening, hate-fueled and derogatory posts, and spoofed or fake accounts to Customer Service.***

For More Information Visit:

- Instagram Help Center
- How to Manage Your Privacy Settings on Social Media

Reminder to State Employees

Complete your mandatory 2019 Security Awareness Training ***Securing the Human*** by **June 3rd.**

Don't Get Hacked

Each time we use social media, we risk the possibility of our accounts being hacked. Follow these tips to harden your account and deter hackers.

Just Log Out

It's the easiest way to keep strangers out of your Instagram account. If you're logged out, it's a lot harder for someone to get in. Logging out after you visit not only protects your security, it also disrupts data collection practices of third-party applications you may have linked to Instagram. This means less targeted advertising!

Use Good Password Hygiene

Do make passwords hard to guess, ***don't*** share them, and ***don't*** use the same one for all social media sites. Set up a calendar reminder to change passwords at least every six months, just like you do for important appointments.

Set up Multi-Factor Authentication

A great way to increase account security is to turn on two -factor/multi-factor authentication. This requires anyone trying to log into your account from any device other than the one you originally registered with Instagram to pass an additional security check. Two-factor authentication requires that you verify your identity with Instagram though email, SMS text message, or another app two ways (via something you know and something you have, such as your phone).

Nix access by third-party applications

Don't allow other apps to use your Instagram or other social media account credentials (in other words, don't "Use [social media account] to log in to [new 3rd party app or website you want to access]". Examples include web apps for games and quizzes that want to use your identity. Create unique identities/logins for new apps/ websites. Malicious apps don't necessarily stop with access to your device's Instagram account but can mine your data and use what they find to access still more of your accounts. If you really feel the need to allow third-party apps, at least research the app via reviews and check legitimacy on other websites.

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

Department of Technology & Information
Delivering Technology that Innovates