January 2020

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Data Privacy in an Era of Compliance

The internet is full of data about you. Whenever you play a game, shop, browse websites, or use any of numerous apps, your activity and some of your personal information may be collected and shared.

Similarly, the business of higher education requires us to collect, process, and store the digital information of others. Whenever we handle such information, we need to think about how we want our own information treated and treat other people's data with the same care and respect.

Protect yourself by following these tips:

- **Know what you are sharing.** Check the privacy settings on all of your social media accounts; some even include a wizard to walk you through the settings. Always be cautious about what you post publicly.
- **Guard your date of birth and telephone number.** These are key pieces of information used for identity and account verification, and you should not share them publicly. If an online service or site asks you to share this critical information, consider whether it is important enough to warrant it.
- **Keep your work and personal presences separate.** Your employer has the right to access your email account, so you should use an outside service for private emails. This also helps you ensure uninterrupted access to your private email and other services if you switch employers.

Continued on page 3...

Inside this issue

Special points of interest

- Additional access may require additional training in Securing the Human; be prepared to finish new modules as they're assigned.
- Keep your eyes out for changes to our security training this year!

Data Privacy Day

Millions of people are uninformed about how their personal information is being used, collected or shared in our digital society. Data Privacy Day, which is recognized on January 28, aims to inspire dialogue and empower individuals and companies to take action.

This year, the National Cyber Security Alliance (NCSA) is encouraging everyone to "Own Your Privacy" by learning more about how to help protect the valuable data that is online. One simple thing you can do is to update your privacy settings by using a helpful tool created by NCSA. You can also follow these tips to create a new "digital you" for the new year:

- **Re-invent yourself with a different online identity.** If a site asks for sensitive, personal information – like your email and/or mailing address, Social Security number, birth date, phone number, etc. – consider "re-inventing" your digital persona by sharing alternative answers to those queries that ONLY you would know. An "alter-internet" persona will help limit tracking by search engines, website and apps. Think of yourself as an actor slipping into a role to help thwart the continuous onslaught of online intrusions. This can also help safeguard you from identity theft.

Continued on page 4...

Data Privacy Day, which is recognized on January 28, aims to inspire dialogue and empower individuals and companies to take action.

California Privacy Law

On Wednesday, January 1, 2020, a new state privacy law took effect in California. The law is known as the California Consumer Privacy Act, or CCPA. The act lays out strict requirements for how data is handled and monetized. Although the law took effect this month, it will not be enforced until July 2020.

This is the most comprehensive law of its kind in the United States. The European Union, with the passage of the General Data Protection Regulation (GDPR) in 2018, is far ahead of the U.S. in privacy law. Europe treats data privacy as a human right, while the U.S. has been lax in its regulation of corporate use of private data.

The CCPA requires companies to disclose what data they collect and how they use the data; it also allows California residents to request that their data not be sold. It applies to companies that have revenue of $25 million or more and that make more than half of their money selling data, and to companies that collect data on 50,000 or more individuals. Companies that violate the CCPA or don't fix violations within 30 days of being notified can be fined up to $7,500 per violation.

There are areas of the law that are fairly broad and open to interpretation, which may create legal battles in its enforcement. For more information about the CCPA, see articles at **www.theverge.com**, **threatpost.com**, and **isc.sans.edu**.

Did You Know?

From CCPA—Quick Overview at **isc.sans.edu**:

The CCPA grants the consumer a right to request…

- specific pieces of information that it collects.
- categories of sources from which that information is collected.
- the business purposes for collecting or selling the information.
- the categories of 3rd parties with which information is shared.
- deletion of personal information…upon receipt of a verified request.

Data Privacy, Con't.

Protect the information, identity, and privacy of others by following these tips:

- **Know what resources are available at your institution.** Colleges and universities might employ individuals with some of the following titles and responsibilities: compliance officer, who can help you navigate the laws and regulations that govern how your institution handles constituents' personal data and what safeguards need to be implemented to ensure the data stay secure; data privacy officer, who can answer questions about how your institution protects the privacy of both your data and constituents' data; and a(n) (chief) information security officer, who can answer questions about information security best practices and the technologies available to protect online identity and the personal data of constituents.
- **Know what policies are in place at your institution.** A privacy policy governs how the institution collects, processes, stores, and deletes the personal data of constituents; a data classification policy governs how the institution organizes the data it interacts with and what rules are in place for processing it; and an information security policy articulates how the institution governs and prioritizes information security activities.
- **Keep constituents' personal information confidential** and limit access to the data.
- **Only use data for its intended purpose.** If you need to use data for another reason, always check relevant resources and policies first for guidance.
- **Destroy or de-identify private information** when you no longer need it.

Resources

- Learn more about data privacy in Higher Education through the EDUCAUSE Understanding Data Privacy Issues in Higher Education Featured Topic Guide.
- Read guidance from the Federal Trade Commission.
- Download NCSA's infographic Your Privacy in a Growing Internet of Me.
- Check out this NCSA infographic: Are You Doing Enough to Protect Consumers' Data?
- See EDUCAUSE's previous Campus Security Awareness Campaign blogs about privacy: January 2018: Privacy is our Shared Responsibility, January 2017: Keep What's Private, Private, January 2016: Guard Your Privacy Online, and February 2016: Guard Your Privacy When Offline or Traveling.

Data Privacy Day, Con't.

- **Share with care.** Be aware that when you post a picture or message, you may also be inadvertently sharing personal details and sensitive data with strangers about yourself, family and friends. It is also OK to limit who can see your information and what you share. Learn about and use privacy and security settings on your favorite websites.
- **Lock down your login.** Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that are easy to remember (for example, "I love country music."). On many sites, you can even use spaces. MFA will fortify your accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device. This additional layer of security makes it harder for bad guys to log in as if they were you.

Note: Text and tips are from the Stay Safe Online website.

The Office of Information Security is responsible for developing and implementing campus-wide policies, controls and procedures to protect the university's information technology resources and systems from intentional or inadvertent modification, disclosure or destruction, as well as monitoring user adherence to these policies.

Longwood University

Information Technology Services
French Hall
201 High Street
Farmville, VA 23909
(434) 395-4357
(434) 395-2034

Fax: (434) 395-2035