

GETTING BACK TO CYBERSECURITY: SECURITY TIPS FOR ONLINE TEACHING & LEARNING



IN COLLABORATION WITH

EDUCAUSE

As colleges and universities prepare for fully online or blended virtual and in-person learning environments, it is important to understand some basic cybersecurity steps students, faculty and staff can take to make sure they move to the top of the class securely.



KNOW YOUR RIGHTS

Under The Family Educational Rights and Privacy Act (FERPA), academic institutions must protect the privacy of student information, including health and academic information. Students can request to see how their information is used.

Learn more about FERPA here:

<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

BEST PRACTICES



THINK BEFORE YOU CLICK

Remember what you learned about not accepting candy from strangers? Apply that to the online world as well. Do not click links in emails, text messages, chat boxes, etc. from people you do not know--and be suspicious of links sent from those you know as well.

If you encounter suspicious messages or attachments, please forward them to the security team at your institution for further investigation. There has been a surge in malicious online activity as cybercriminals and cyberattackers leverage the heightened fear of the public during the coronavirus pandemic.



PROTECT YOUR PERSONAL INFORMATION

Personal information is any information that can be used to identify you or your accounts. Examples include your name, address, phone number, usernames and passwords, pictures, birthday and social security number. Don't post or share this information with others.



CyberSecurity4biz.com

can your business survive without its data?

GETTING BACK TO CYBERSECURITY: SECURITY TIPS FOR ONLINE TEACHING & LEARNING



IN COLLABORATION WITH

EDUCAUSE

BEST PRACTICES



PROTECT YOUR COMPUTER

Be sure to keep your laptop or tablet close to you. When you're done using it for the day, put it in a safe place at home. Don't leave it by itself outside or in a public place.



USE A PASSWORD MANAGER

Because there are a lot more threats out there during the pandemic, there are plenty of bad actors looking to take over accounts. The easiest way to protect your accounts from being compromised is to use long, complex, and unique passwords and the easiest way to do that is to use a password manager.



EMPLOY MFA

Double down on your account security with multi-factor authentication (MFA). MFA adds a second check to verify your identity when logging in to one of your accounts. This helps to keep your account from being compromised even if your password falls into the wrong hands.



DON'T HESITATE TO UPDATE

Having the latest security software, web browser, and operating system on devices is one of the best defenses against online threats. When the computer or device says it's time to update the software, don't click postpone. Update.



RUN YOUR ANTIVIRUS SOFTWARE

Find out if your university provides antivirus software. Most universities equip employee computers with antivirus software and some also make antivirus software available online for download on your home computer. You can usually get this information from the IT help desk or the campus security team.



CyberSecurity4biz.com

can your business survive without its data?

GETTING BACK TO CYBERSECURITY: SECURITY TIPS FOR ONLINE TEACHING & LEARNING



IN COLLABORATION WITH

EDUCAUSE

BEST PRACTICES



APPLY YOUR RESEARCH SKILLS

Apps are a great way to learn and apply knowledge. Before downloading any new learning app on your device, make sure it's a legitimate app. Who created the app? What do the user reviews say? Are there any articles published online about the app's privacy & security features (or lack thereof)?



MAINTAIN A SECURE WORKSTATION

Use institution-issued devices for all your work so you can take advantage of security controls built in by your IT and security teams. If you would like to find out what settings to toggle on or off to secure your workflow and data on your college/university machine, please contact your respective IT and/or security department for advice.



MAINTAIN A CLEAN WORKSPACE

If you're using a shared workspace, be conscious of clearing it of sensitive, nonpublic information, especially if you have to step away. Also, avoid printing out sensitive information at home or in public spaces if it's not necessary. In addition, if you are listening in on or participating in meetings that could be considered sensitive or in which you share nonpublic information, be sure to put on headphones.



CONFIGURE YOUR SETTINGS

Whether you are teaching or learning in a new platform, take a moment to explore the privacy and security settings to limit disruptions and improve the experience. For example, create passwords so only those invited to the session can attend. Another example would be to restrict who can share their screen or files with the rest of the group. If you need help, reach out to your school's IT & security team or instructional design team for help.



CyberSecurity4biz.com

can your business survive without its data?

GETTING BACK TO CYBERSECURITY: SECURITY TIPS FOR ONLINE TEACHING & LEARNING



IN COLLABORATION WITH

EDUCAUSE

LEARN MORE

- Multi-Factor Authentication**
<https://er.educause.edu/blogs/2018/12/may-2019-2fa-control-in-the-palm-of-your-hand>
- Password-Managers**
<https://library.educause.edu/resources/2015/7/password-managers>
- Information Security guide**
<https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide>
- Security Awareness Videos**
<https://staysafeonline.org/resource/security-awareness-episodes/>



The National Cyber Security Alliance (NCSA) builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work and school with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity. www.staysafeonline.org

EDUCAUSE

EDUCAUSE is a community of IT leaders and professionals working together to tackle challenges and leverage opportunities that are constantly evolving within higher education. EDUCAUSE welcomes diversity, in viewpoints and experience, and believes in the transformative power of uncommon thinking for the common good. Visit <http://educause.edu/>



CyberSecurity4biz.com

can your business survive without its data?