12 back-to-school cybersecurity tips for parents

James J. Giszczak, Amanda Rose Martin | Tuesday, August 27, 2019

Back-to-school season is in full swing, and with technology and education so intertwined these days it's more likely your student will be logging on to a laptop or tablet then cracking open a textbook. Whether your little one just started kindergarten or is finishing up at college, data privacy and cybersecurity preparedness should be top of mind for all parents throughout the school year. McDonald Hopkins' national Data Privacy and Cybersecurity team has prepared 12 tips for parents on how to keep your children safe and your information protected.

1. **Review your school's information policy.** It is important to review your school's information policy so you know what personal information about your student they may or may not be sharing. Provided they give public notice (in a student handbook or newsletter, for example), schools are allowed to disclose "directory information" to third parties

without notifying a parent or student individually. “Directory information" can include name, address, telephone number, date and place of birth, participation in sports or extracurricular activities, and dates of attendance. Under the Family Educational Rights and Privacy Act (FERPA), you have the right to control the disclosure over some of this personal information and should consider whether you would like this information available. If not, you may notify your student’s school that you do not want this information disclosed.

2. **Keep up to date on what is going on.** Keep up-to-date on what is happening at school and in your child’s classroom – read every notice and newsletter you get and subscribe to the school’s official social media feeds. That way you won’t be caught off guard by an unexpected email or call that seems like it is coming from the school or your child’s teacher. Never open an email or attachment from an untrusted source or give personal information over the phone without verifying the caller is legitimate. Phishing is a very common technique where scammers pose as a company you know and trust and then use email, phone calls or text messages to trick people into giving them personal information like account numbers, Social Security numbers or passwords.
3. **Transmit online information securely.** Whether paying tuition or adding to your student’s school lunch account, make sure the website you’re using to transmit any banking or personal information is secure. Secure websites start with “https” or have

the lock symbol in the address bar. If you have questions, call your school and ask about their network. If you receive a suspicious email from your students' school noting that payment methods have changed, always call a known number to verify.

4. **Beware of public Wi-Fi.** Coffee shops and student unions can be prime hunting grounds for cyber criminals because it is much easier for them to steal personal and financial information that is shared over public Wi-Fi. Remind your student that if they have to access personal or financial information while out, they should consider using a VPN or their cellular signal instead. Protecting that personal information is worth using up your data plan. Also, beware that after using public Wi-Fi and coming home to connect with your private network, your student could bring home malware that could infect your other computers or devices.
5. **Protect personal information.** If you're wondering why a certain registration form or permission slip is asking for specific information like a Social Security Number or any other personal information, ask. You may be able to opt- out of providing the information. Also, talk to your student about what type of sensitive information they may be inadvertently posting online – think videos or photos that could include the location of valuables or a home address in the background or a screenshot that includes a private phone number.
6. **Check used devices for malware.** If you're operating on a budget or wary of spending big bucks on a new device for your student, be cautious of used devices. These can be infected with malware or other programs that could potentially steal your information.

When purchasing used devices, it's recommended you wipe them using professional software or reset them to factory defaults before using.

7. **Properly dispose of your old devices.** If you've upgraded your student with a new device, make sure to take the right steps before throwing away (or recycling, reselling, donating) their old device. Back up whatever information you want to save, then wipe the machine clean of any personal data using a program that will truly wipe all data from the device. Just deleting the data will not remove it from the device. You should also remove the SIM card or hard drive. If you have an Apple device that you've already gotten rid of, there are even steps you can take to remotely wipe everything. Your best bet is to have a company that specializes in erasing data from devices take care of this for you. There are also companies that will shred your hard drive.
8. **Keep in mind physical security.** Many data breaches are caused by the physical theft of devices left unattended or unsecure. Purchase locking cables or USB port blockers for your student and remind them to never leave their devices unattended. When they do have to walk away from their device, remind your student to lock their screen. And talk to them about being cognizant of shoulder surfing –when someone looking over your shoulder at your screen steals your information.
9. **Back up your data.** By saving important information and backing up your data on an external hard drive or cloud-based account you give yourself some protection from a ransomware attack. Ransomware is one of the most common types of data security

incidents, and often unfolds in the same way: after being deployed by attackers, the ransomware encrypts files on a system so that they are inaccessible. A ransom note left by the attackers provides contact information and a promise to provide a decryption key – for a price of course, and it is likely one you or your student isn't going to want to pay.

10. **Watch out for video game and app activity.** Online gaming and popular apps have exposed kids to a whole new level of hacking and cybercrime. Without even realizing it, your student could be sharing personal information on gaming forums, talking to dangerous cybercriminals on chats, or making purchases with your banking information on unsecure sites.
11. **Monitor the activity on your work device.** It is best to avoid this practice altogether, but if you let your student use your work laptop or mobile device for homework or research, make sure you monitor their online activity. Talk to them about what they can or can not use the device for and never let them set up accounts or save personal information on the device. By letting your child use a work device, you are opening yourself up to the risk of a data breach that impacts not just you but your entire company.
12. **Don't forget the basics.** Don't forget to apply the data security practices that you already know to the new school year. When receiving an unexpected email, even if it's purportedly from your student's school or teacher, don't click on any links or download any documents until you verify the source. Talk to your student about using strong passwords and, where applicable, multi-factor authentication. Make sure that you and your student keep

your programs and apps up to date, especially on any internet-accessible devices, to ensure that you are applying the strongest security to your personal information.

For questions or more information about keeping your information protected throughout the school year, contact one of the attorneys listed below or any member of our **national data privacy and cybersecurity team**.

James J. Giszczak

Team member bio

Amanda Rose Martin

Team member bio