Since a wide array of different social media outlets have become so popular for people of all ages, in recent years children—including some of my fictional characters—have become increasingly vulnerable targets for hacks of one kind or another.

Hacking for Good and Bad, and How to Protect Yourself against Hacks!

Barnas Monteith
bmonteith@tumblehomelearning.com

As a founder and former head of a Boston-based IT company and, subsequently, as a person who has continued to work in both software and hardware-driven technology fields, I've seen plenty of "hacks" in my days. From viruses that would send playful—yet annoying—messages to worms that would wipe out an entire corporate network's (or government network's) data, hacks can be anything from localized nuisances to major economic disasters.

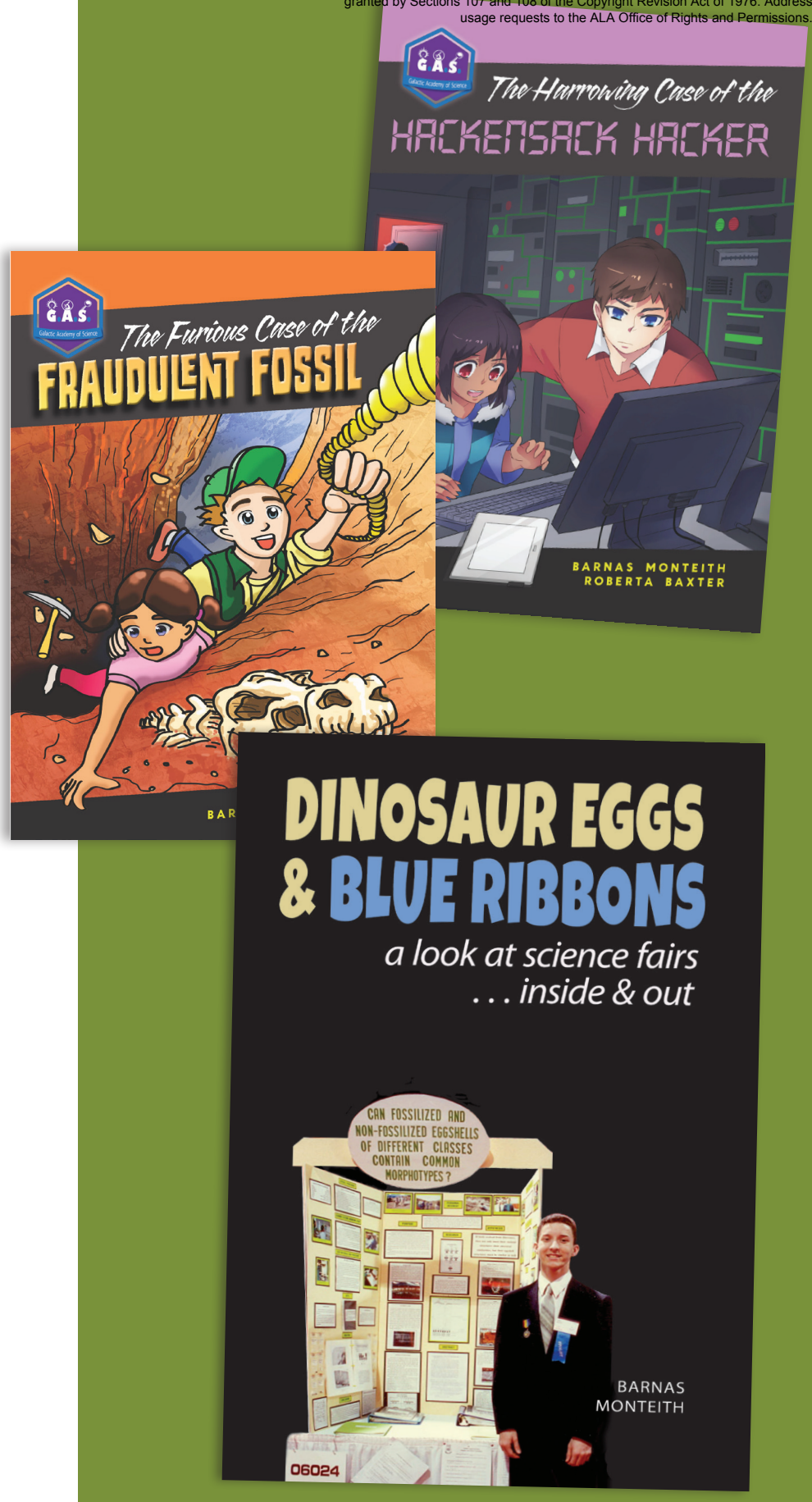
In the late 1990s, after having earlier been recognized as one of the top winning science fair participants in the U.S. for projects on fossil eggshell paleobiochemistry and then being formally trained in biology, geology, and related fields for an intended career in paleontology, I never expected to end up working in the fields of computers, software, and semiconductor materials. (Of course, I also didn't imagine that later on I'd become a children's book writer and artist.) But, there I was, in the early summer of 1998—a scrawny, nerdy kid who had about eight years of formal and informal paleobiochemistry and field paleontology training. I'd recently won recognition as one of the youngest people ever to present a plenary session lecture at the world's biggest paleontology convention and with research sponsored by both Tufts and Harvard. That summer I should have been looking at paleontology grad schools. Yet, despite all the summers in Montana, Arizona, Utah, and Canada, and countless afternoons in microscopy, biochem, and fossil-preparation labs throughout eastern Massachusetts, I still found myself logging more hours in front of a computer—as I had over the previous years—rather than wielding a rock hammer. (As a result of my combo of interests, nearly all of my books are about fossils, computers, and science fairs!)

Around the time I considered paleontology grad schools, I also found myself looking at ways to find venture capital to start a company

specializing in IT and security. At that point I had about ten years of database training, starting with a middle school program in C+ I took at MIT. Several of my friends had mentioned to me how "easy" it was to get capital, and I decided I might as well try. This was the era of the dot.com boom (documented by the movie *Startup.com*, which I highly recommend). Although at first I didn't believe my friends, after a few elevator pitches at local business competitions and within about a year of getting my bachelor's degree, I found myself with a few dozen employees, a corner office, a "high speed T1" connection, a roomful of servers, and perhaps a hundred clients. And the business kept growing—but my path never really turned out as I expected.

My intention had been to stay on the bleeding edge of technology, leading teams of people to make productive database-driven software running financial, insurance, and government apps (and maybe do some paleontology/evolution side projects for fun). However, instead I found myself spending a great deal of time simply keeping up with the daily hacks that would hit my various clients' and my own servers. As the 1990s transitioned into the 2000s, I realized that this state would become the norm. The Internet was changing business as everybody knew it—for both good and bad reasons.

What had been kind of funny in the past had become something scary and taboo even to discuss, lest you be labeled a hacker.



Hacking had become a tool for personal, corporate, and government espionage, and, ultimately, even military and terrorist operations. The term no longer referred to innocent pranks on par with those conducted regularly at MIT in an earlier era, such as disassembling and reassembling a police car on top of the main dome at MIT. What had been kind of funny in the past had become something scary and taboo even to discuss, lest you be labeled a hacker. Over the years, the distinction between "white hat" (hackers for good) and "black hat" (malicious) hackers has emerged, and, at times, distinguishing between the two has become hard. Hacker military forces, mercenary hackers, and corporate hackers for hire have been exposed in recent years, and the field is ever expanding.

Hacking and Kids

Since a wide array of different social media outlets have become so popular for people of all ages, in recent years children—including some of my fictional characters—have become increasingly vulnerable targets for hacks of one kind or another. Therefore, I believe it is very important that children are maximally protected at home, at school, at libraries, and all other places where they may be exposed to the reach of the "black hat." As a result, some of my IT-related work, as well as some of my writing, is intended to help protect children and to help them protect themselves.

When I'm doing talks and presentations at schools, the question children ask me most often is: "So, is hacking good or bad?" It is an incredibly difficult question to answer, since it's hard to justify breaking laws or violating personal privacy for the sake of "good." Clearly, when malicious hackers steal money or engage in identity theft, they are doing something that everyone except the hackers considers to be bad, but should all hacking be considered bad as a result of this malicious behavior? Even when governments or police forces use hacking to help save lives? Students often have interesting perspectives to contribute to the discussion.

Readers of my novel *The Harrowing Case of the Hackensack Hacker* learn some of the history of hacking and the intentions and plans of early hackers. Though it is fiction, it's in Tumblehome Learning's Galactic Academy of Science series, so science and engineering principles are covered as well. And, in the end, the good guys win. Sorry, but I can't tell you more; you can, of course, read the book!

Since this book came out in 2013, I've visited a number of schools and libraries and explained to children the basic concepts of hacking. By hacking a simple LOGO-like program that does nothing more than change graphics on a monitor, I make hacking visible to kids. (For more about this hack, read the supplementary material at the back of *The Harrowing Case of the Hackensack Hacker*, contributed by Bob Tinker, founder of the Concord Consortium.) The demo is an excellent starting point for a discussion about ethical use of technology and about the importance of basic personal security and privacy.

Tips for Tech Users of All Ages

In general, tech users of all ages should follow a number of rules to ensure that social media accounts, e-mail accounts, and home computers remain (at least mostly) hack-proofed! The most common reason people's devices get hacked is because they haven't followed these guidelines and done simple—but essential—tasks.

1. Make sure your passwords are not something obvious. Please include numbers, capitals, and special characters when you can, and change passwords very regularly (monthly or more frequently). Store passwords off-line, and off-computer, in an area nobody but you will *ever* find!

2. Protect yourself when you are on school, library, or other public computers. When you log into your Facebook, Twitter, Pinterest, and other social media and e-mail accounts on public devices, *always* click "No" when the browser asks whether to save your password. Before you leave the public computer, in addition to checking that you have your wallet, keys, jacket, backpack, etc., be sure you have logged out *every* time.

3. Protect your personal devices by installing—and frequently updating—anti-malware and anti-virus software from a reliable source.

4. Keep your computer and phone access malware-free. Don't click on links or open e-mails or attachments from people or sources you don't know. Don't download software unless you are absolutely sure it does not contain viruses. Typically, this means downloading only from major companies and only after you've confirmed online that these particular releases/versions do not harbor potential problems.

While following these simple rules won't 100 percent ensure that you won't get viruses, malware, worms, or other terrible computer pathogens indicative of a hack, you'll have taken important steps to protect yourself.

Barnas Monteith *is chairman of Massachusetts State Science & Engineering Fair, Inc., one of the oldest inquiry-based science education nonprofits in the U.S. Barnas is the most successful Massachusetts science fair participant in history, with a record of eight first-place MA wins, and numerous first-place awards at the national and international levels. His projects focused on computerized models to study evolution, work that he continued at both Tufts and Harvard. He started several successful technology companies in the fields of wearable computing, financial and security software development, and semiconductor research and development, specializing in diamonds, renewable energy, and lighting. He serves on the Massachusetts Department of Elementary and Secondary Education Math and Science Advisory Council and was a gubernatorial appointee to the Massachusetts governor's STEM Advisory Council, serving as a committee cochair. He has coauthored several patents, published a number of scientific articles, and speaks regularly at global STEM events. Among his recent children's books published by Tumbledown Learning are* The Furious Case of the Fraudulent Fossil *(2012),* The Harrowing Case of the Hackensack Hacker *(2013), and* Dinosaur Eggs and Blue Ribbons *(2015).*

Statement of Ownership and Management

Knowledge Quest, Publication No. 483-860, is published five times per year by the American Association of School Librarian, American Library Association, 50 E. Huron St., Chicago, IL 60611-2795. Annual subscription price, $50. Printed in U.S.A. with periodical class postage paid at (Illinois). As a nonprofit organization authorized to mail at special rates (DMM Section 424.12 only), the purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes have not changed during the preceding twelve months.

Extent and Nature of Circulation

("Average" figures denote the average number of copies printed each issue during the preceding twelve months; "actual" figures denote actual number of copies of single issue published nearest to filing date: September/October 2015 issue). Total number of copies printed average 7,798; actual 8,175. Sales through dealers, carriers, street vendors, and counter sales: none. Mail subscription: actual 6,631. Free distribution actual 294. Total distribution average 7,798; actual 8,175. Office use, leftover, unaccounted, spoiled after printing average 614; actual 1,250. Total: average/actual 7,798/ 8,175. Percentage paid: average 95.7; actual 95.7.

INDEX TO ADVERTISERS