Summer 2019

engage

LIVE WITH PURPOSE

Summer 2019 newsletter of the North Shore Senior Center, Northfield, IL

CYBERBSECURITY

Requires

Careful Attention to Potential Threats

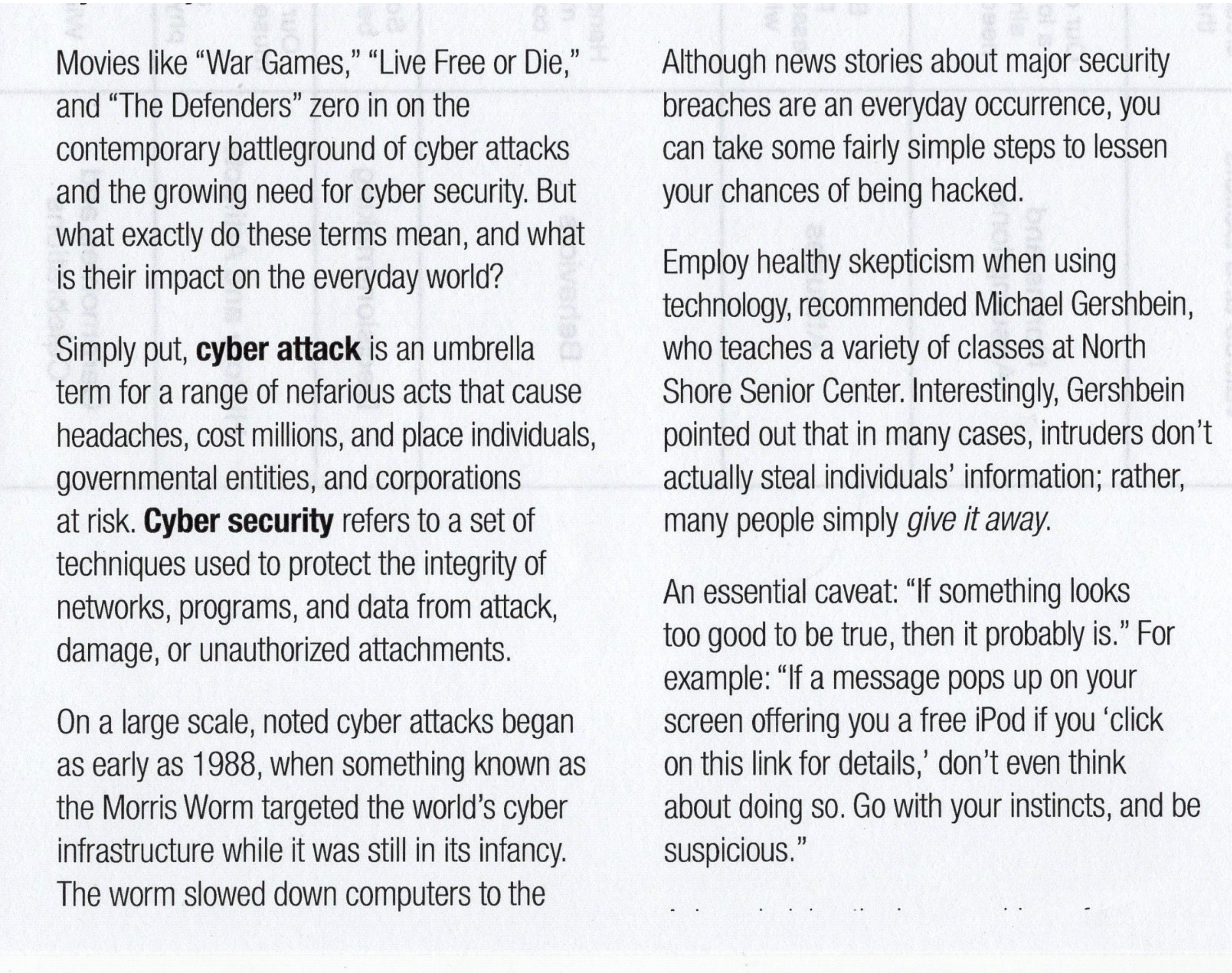
by Betsy Storm

Reduce Your Likelihood of Being SCAMMED

by Betsy Storm

It sounds all wrong, and *it is*: The words "grandparent" and "scam" don't belong in the same sentence. But nonetheless, "grandparent scams" or "elder scams" are a persistent problem. The National Council on Aging refers to such fraudulent activities as "the crime of the 21st Century." The cost of financial fraud affecting older adults is estimated to be $3 million and growing, according to the Federal Trade Commission.

(continued on page 5)



Movies like "War Games," "Live Free or Die," and "The Defenders" zero in on the contemporary battleground of cyber attacks and the growing need for cyber security. But what exactly do these terms mean, and what is their impact on the everyday world?

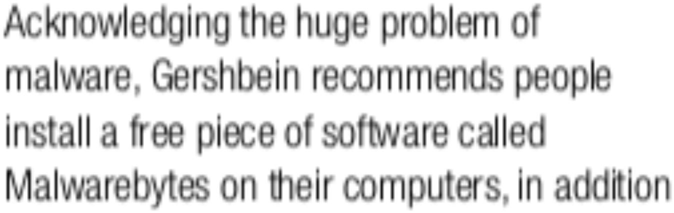
Simply put, **cyber attack** is an umbrella term for a range of nefarious acts that cause headaches, cost millions, and place individuals, governmental entities, and corporations at risk. **Cyber security** refers to a set of techniques used to protect the integrity of networks, programs, and data from attack, damage, or unauthorized attachments.

On a large scale, noted cyber attacks began as early as 1988, when something known as the Morris Worm targeted the world's cyber infrastructure while it was still in its infancy. The worm slowed down computers to the

Although news stories about major security breaches are an everyday occurrence, you can take some fairly simple steps to lessen your chances of being hacked.

Employ healthy skepticism when using technology, recommended Michael Gershbein, who teaches a variety of classes at North Shore Senior Center. Interestingly, Gershbein pointed out that in many cases, intruders don't actually steal individuals' information; rather, many people simply *give it away*.

An essential caveat: "If something looks too good to be true, then it probably is." For example: "If a message pops up on your screen offering you a free iPod if you 'click on this link for details,' don't even think about doing so. Go with your instincts, and be suspicious."



Acknowledging the huge problem of malware, Gershbein recommends people install a free piece of software called Malwarebytes on their computers, in addition to their computer's antivirus program. The developer of Malwarebytes claims to "use layers of technology like anomaly detection (a cool sort of artificial intelligence), behavior matching, and application hardening to crush malware that hasn't even been seen before." Versions are also available for PC, for business, and with a paid subscription (more features).

Detective Steve Gilmour of the Northfield Police Department echoed Gershbein's advice. Gilmour said suspicious emails are a major problem and admitted that even he has to resist opening some particularly tempting messages: "Dangerous emails can be very well-disguised."

Gilmour also warns against having unprotected (no password) Wi-Fi at home. Unbeknownst to you, he explains, a cyber thief can drive around a neighborhood, find an unsecured account, and access it to break into an individual's accounts and possibly even steal confidential financial information.

Gilmour said another problem is phishing-type phone calls. He added, in particular, that seniors are often scammed by callers that claim a grandchild or other family member is in trouble and needs money (see related story on page 4). Odd though it seems, says Gilmour, these criminals often ask for currency in the form of gift cards because gift cards can't be tracked (they are usable as long as the serial number on them is available). The person on the receiving end of the call often panics, said

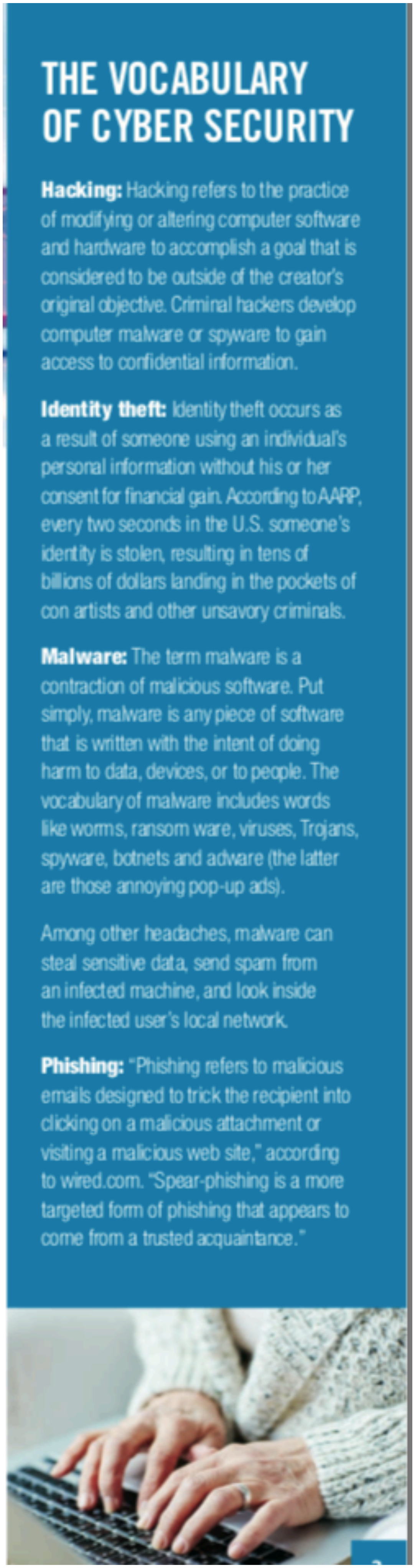
Gilmour, and the scammers get what they want by preying on seniors' concerns for their family members.

Here are a few tips from a security-sawy North Shore Senior Center member who we will call "Annie" to protect her privacy. Annie said being vigilant on a daily basis pays off. When traveling, she carries only one credit card and alerts her credit card company of her itinerary in advance. As a result, the company can monitor any unusual activity on her accounts. Annie has also set up alerts with her banks and other financial services companies; *anytime* there's activity on her accounts, she receives an alert. And because Annie has frozen her credit reports on the "big three" credit monitoring companies, she is quickly notified if anyone starts poking around in her credit history.

Copious amounts of expertise are available to help you stay secure. Two well-reviewed books are: "Senior Online Safety: Useful Tips to Stay Safe and Secure for Seniors, Both Online and Off" by Christopher Burgess and "My Internet for Seniors" by Michael Miller. AARP.com is a storehouse of information, as are Michael Gershbein's classes at the Center.

Using the aforementioned resources, focus on learning how to:

- create secure passwords
- back up your data
- keep personal information personal
- guard against email scams
- protect yourself from malware



THE VOCABULARY OF CYBER SECURITY

Hacking: Hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Criminal hackers develop computer malware or spyware to gain access to confidential information.

Identity theft: Identity theft occurs as a result of someone using an individual's personal information without his or her consent for financial gain. According to AARP, every two seconds in the U.S. someone's identity is stolen, resulting in tens of billions of dollars landing in the pockets of con artists and other unsavory criminals.

Malware: The term malware is a contraction of malicious software. Put simply, malware is any piece of software that is written with the intent of doing harm to data, devices, or to people. The vocabulary of malware includes words like worms, ransom ware, viruses, Trojans, spyware, botnets and adware (the latter are those annoying pop-up ads).

Among other headaches, malware can steal sensitive data, send spam from an infected machine, and look inside the infected user's local network.

Phishing: "Phishing refers to malicious emails designed to trick the recipient into clicking on a malicious attachment or visiting a malicious web site," according to wired.com. "Spear-phishing is a more targeted form of phishing that appears to come from a trusted acquaintance."