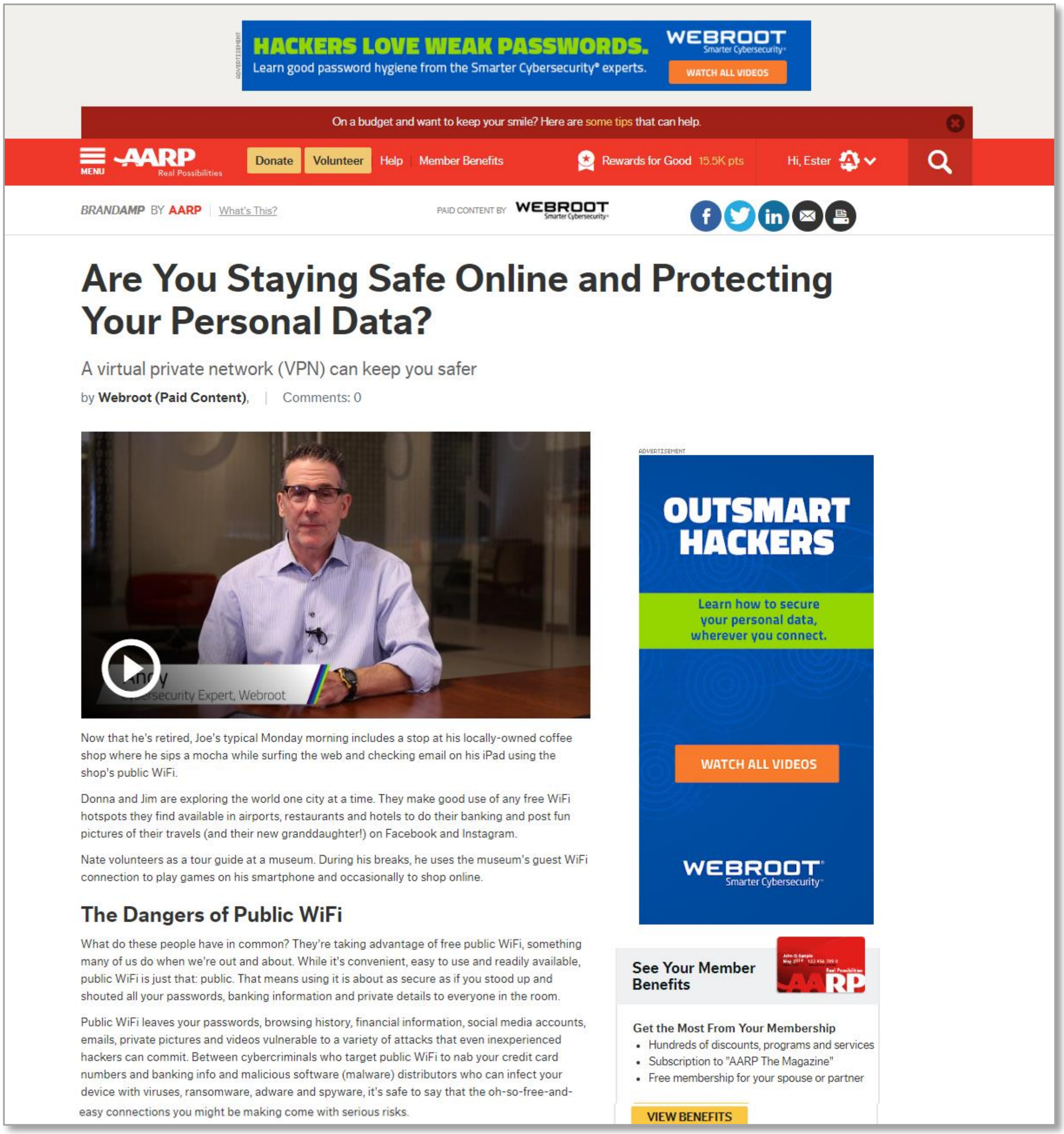
Q4 2018



ADVERTISEMENT
HACKERS LOVE WEAK PASSWORDS.
Learn good password hygiene from the Smarter Cybersecurity® experts.
WEBROOT Smarter Cybersecurity
WATCH ALL VIDEOS
On a budget and want to keep your smile? Here are some tips that can help.
MENU
AARP Real Possibilities
Donate
Volunteer
Help
Member Benefits
Rewards for Good 15.5K pts
Hi, Ester
BRANDAMP BY AARP
What's This?
PAID CONTENT BY WEBROOT
Andy
Cybersecurity Expert, Webroot
ADVERTISEMENT
OUTSMART HACKERS
Learn how to secure your personal data, wherever you connect.
WATCH ALL VIDEOS
WEBROOT Smarter Cybersecurity

Are You Staying Safe Online and Protecting Your Personal Data?

A virtual private network (VPN) can keep you safer

by **Webroot (Paid Content)**, | Comments: 0

Now that he's retired, Joe's typical Monday morning includes a stop at his locally-owned coffee shop where he sips a mocha while surfing the web and checking email on his iPad using the shop's public WiFi.

Donna and Jim are exploring the world one city at a time. They make good use of any free WiFi hotspots they find available in airports, restaurants and hotels to do their banking and post fun pictures of their travels (and their new granddaughter!) on Facebook and Instagram.

Nate volunteers as a tour guide at a museum. During his breaks, he uses the museum's guest WiFi connection to play games on his smartphone and occasionally to shop online.

The Dangers of Public WiFi

What do these people have in common? They're taking advantage of free public WiFi, something many of us do when we're out and about. While it's convenient, easy to use and readily available, public WiFi is just that: public. That means using it is about as secure as if you stood up and shouted all your passwords, banking information and private details to everyone in the room.

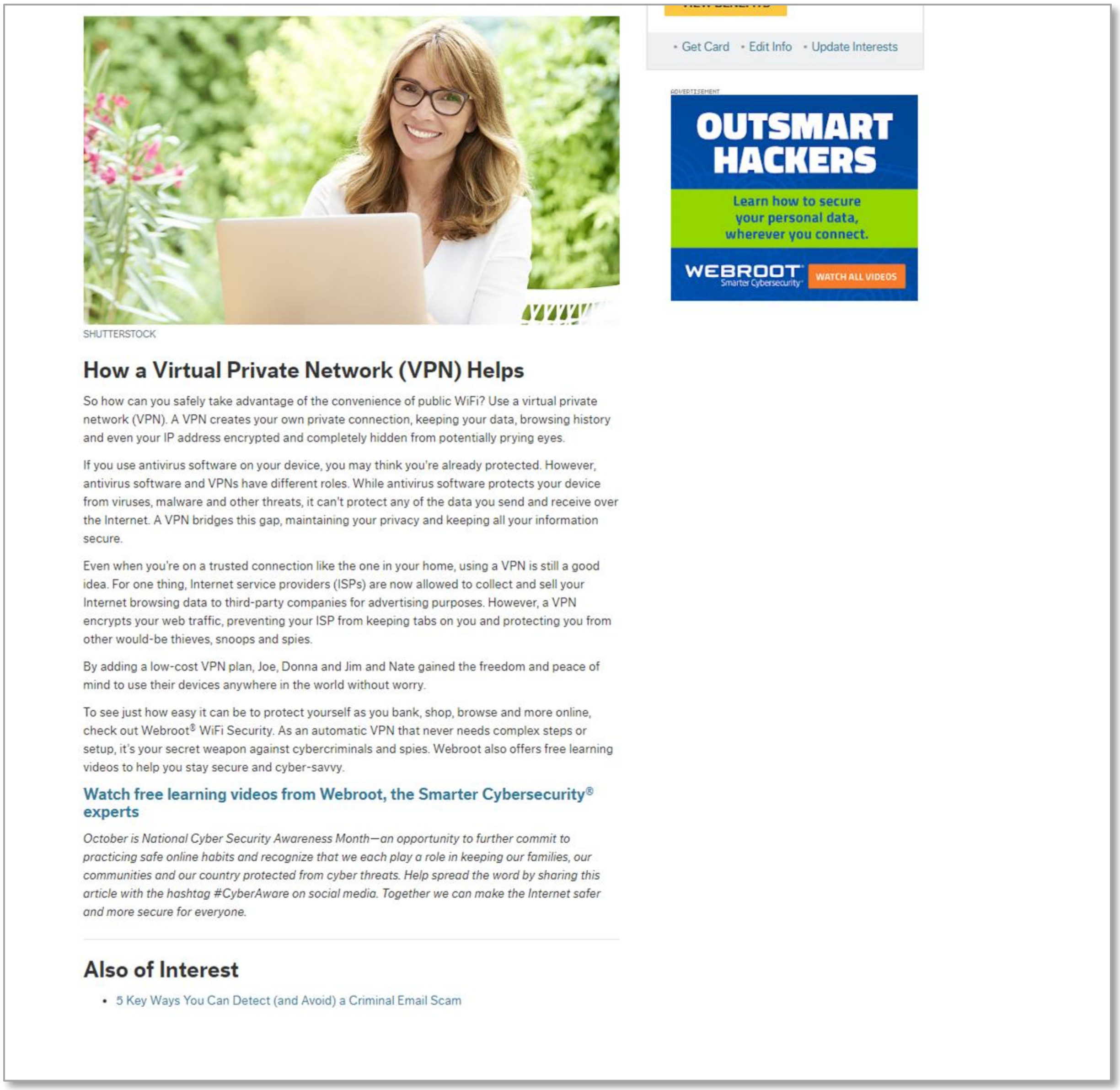
Public WiFi leaves your passwords, browsing history, financial information, social media accounts, emails, private pictures and videos vulnerable to a variety of attacks that even inexperienced hackers can commit. Between cybercriminals who target public WiFi to nab your credit card numbers and banking info and malicious software (malware) distributors who can infect your device with viruses, ransomware, adware and spyware, it's safe to say that the oh-so-free-and-easy connections you might be making come with serious risks.

See Your Member Benefits

Get the Most From Your Membership

- Hundreds of discounts, programs and services
- Subscription to "AARP The Magazine"
- Free membership for your spouse or partner

VIEW BENEFITS



• Get Card • Edit Info • Update Interests

SHUTTERSTOCK

How a Virtual Private Network (VPN) Helps

So how can you safely take advantage of the convenience of public WiFi? Use a virtual private network (VPN). A VPN creates your own private connection, keeping your data, browsing history and even your IP address encrypted and completely hidden from potentially prying eyes.

If you use antivirus software on your device, you may think you're already protected. However, antivirus software and VPNs have different roles. While antivirus software protects your device from viruses, malware and other threats, it can't protect any of the data you send and receive over the Internet. A VPN bridges this gap, maintaining your privacy and keeping all your information secure.

Even when you're on a trusted connection like the one in your home, using a VPN is still a good idea. For one thing, Internet service providers (ISPs) are now allowed to collect and sell your Internet browsing data to third-party companies for advertising purposes. However, a VPN encrypts your web traffic, preventing your ISP from keeping tabs on you and protecting you from other would-be thieves, snoops and spies.

By adding a low-cost VPN plan, Joe, Donna and Jim and Nate gained the freedom and peace of mind to use their devices anywhere in the world without worry.

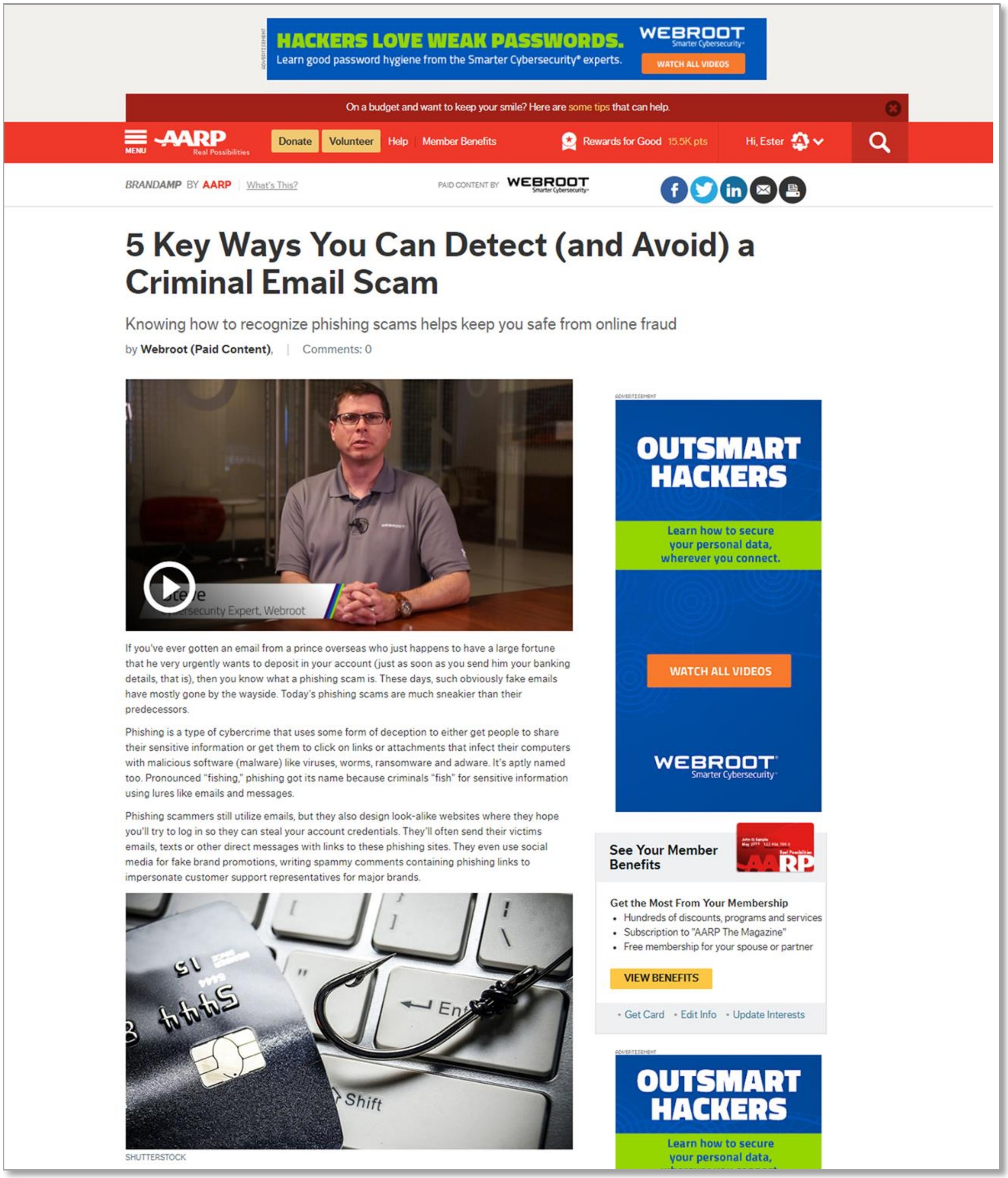
To see just how easy it can be to protect yourself as you bank, shop, browse and more online, check out Webroot® WiFi Security. As an automatic VPN that never needs complex steps or setup, it's your secret weapon against cybercriminals and spies. Webroot also offers free learning videos to help you stay secure and cyber-savvy.

Watch free learning videos from Webroot, the Smarter Cybersecurity® experts

October is National Cyber Security Awareness Month—an opportunity to further commit to practicing safe online habits and recognize that we each play a role in keeping our families, our communities and our country protected from cyber threats. Help spread the word by sharing this article with the hashtag #CyberAware on social media. Together we can make the Internet safer and more secure for everyone.

Also of Interest

- 5 Key Ways You Can Detect (and Avoid) a Criminal Email Scam



On a budget and want to keep your smile? Here are some tips that can help.

5 Key Ways You Can Detect (and Avoid) a Criminal Email Scam

Knowing how to recognize phishing scams helps keep you safe from online fraud

by **Webroot (Paid Content)**, | Comments: 0

If you've ever gotten an email from a prince overseas who just happens to have a large fortune that he very urgently wants to deposit in your account (just as soon as you send him your banking details, that is), then you know what a phishing scam is. These days, such obviously fake emails have mostly gone by the wayside. Today's phishing scams are much sneakier than their predecessors.

Phishing is a type of cybercrime that uses some form of deception to either get people to share their sensitive information or get them to click on links or attachments that infect their computers with malicious software (malware) like viruses, worms, ransomware and adware. It's aptly named too. Pronounced "fishing," phishing got its name because criminals "fish" for sensitive information using lures like emails and messages.

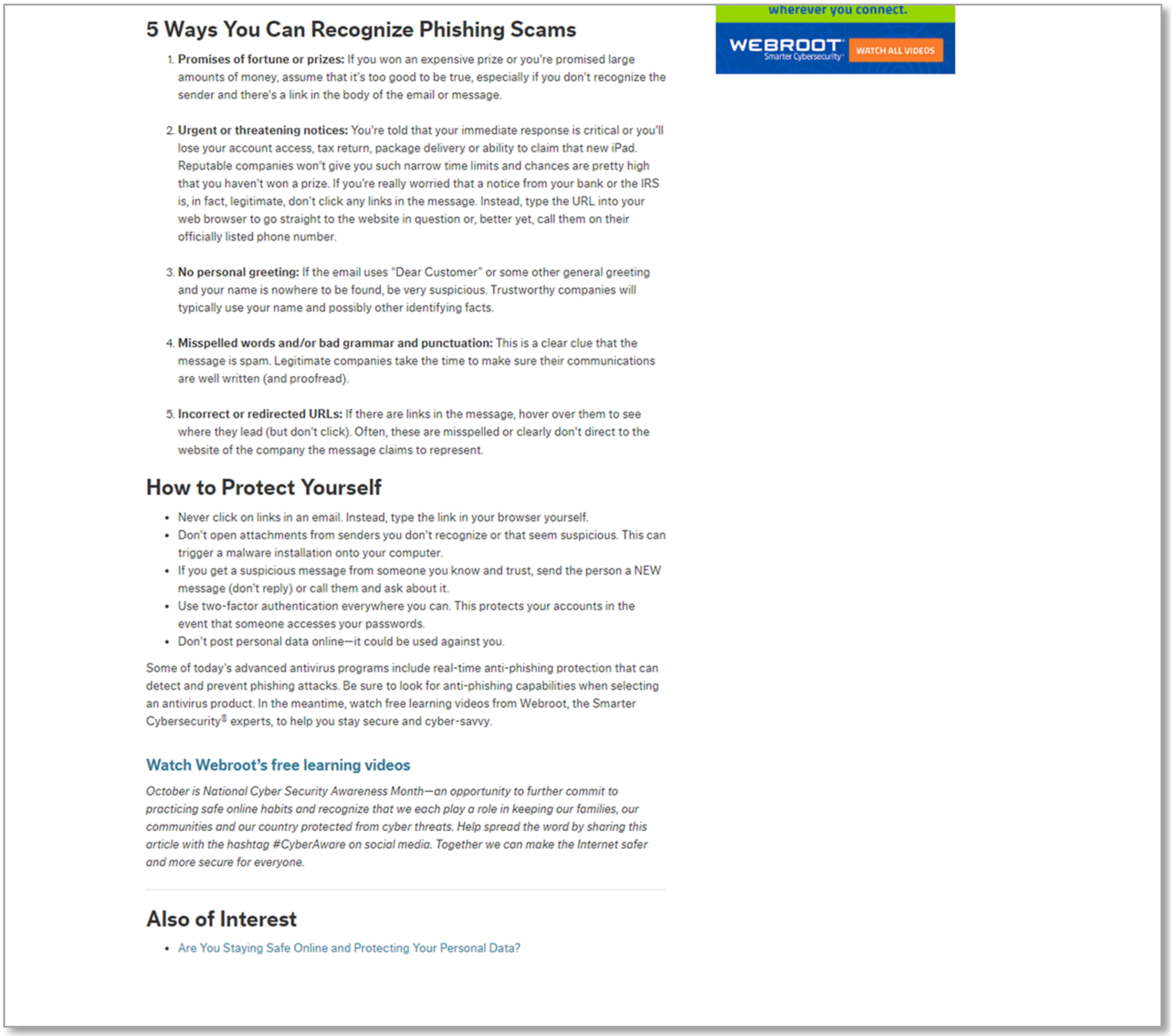
Phishing scammers still utilize emails, but they also design look-alike websites where they hope you'll try to log in so they can steal your account credentials. They'll often send their victims emails, texts or other direct messages with links to these phishing sites. They even use social media for fake brand promotions, writing spammy comments containing phishing links to impersonate customer support representatives for major brands.

SHUTTERSTOCK

See Your Member Benefits

Get the Most From Your Membership

- Hundreds of discounts, programs and services
- Subscription to "AARP The Magazine"
- Free membership for your spouse or partner



5 Ways You Can Recognize Phishing Scams

1. **Promises of fortune or prizes:** If you won an expensive prize or you're promised large amounts of money, assume that it's too good to be true, especially if you don't recognize the sender and there's a link in the body of the email or message.

2. **Urgent or threatening notices:** You're told that your immediate response is critical or you'll lose your account access, tax return, package delivery or ability to claim that new iPad. Reputable companies won't give you such narrow time limits and chances are pretty high that you haven't won a prize. If you're really worried that a notice from your bank or the IRS is, in fact, legitimate, don't click any links in the message. Instead, type the URL into your web browser to go straight to the website in question or, better yet, call them on their officially listed phone number.

3. **No personal greeting:** If the email uses "Dear Customer" or some other general greeting and your name is nowhere to be found, be very suspicious. Trustworthy companies will typically use your name and possibly other identifying facts.

4. **Misspelled words and/or bad grammar and punctuation:** This is a clear clue that the message is spam. Legitimate companies take the time to make sure their communications are well written (and proofread).

5. **Incorrect or redirected URLs:** If there are links in the message, hover over them to see where they lead (but don't click). Often, these are misspelled or clearly don't direct to the website of the company the message claims to represent.

How to Protect Yourself

- Never click on links in an email. Instead, type the link in your browser yourself.
- Don't open attachments from senders you don't recognize or that seem suspicious. This can trigger a malware installation onto your computer.
- If you get a suspicious message from someone you know and trust, send the person a NEW message (don't reply) or call them and ask about it.
- Use two-factor authentication everywhere you can. This protects your accounts in the event that someone accesses your passwords.
- Don't post personal data online—it could be used against you.

Some of today's advanced antivirus programs include real-time anti-phishing protection that can detect and prevent phishing attacks. Be sure to look for anti-phishing capabilities when selecting an antivirus product. In the meantime, watch free learning videos from Webroot, the Smarter Cybersecurity® experts, to help you stay secure and cyber-savvy.

Watch Webroot's free learning videos

October is National Cyber Security Awareness Month—an opportunity to further commit to practicing safe online habits and recognize that we each play a role in keeping our families, our communities and our country protected from cyber threats. Help spread the word by sharing this article with the hashtag #CyberAware on social media. Together we can make the Internet safer and more secure for everyone.

Also of Interest

- Are You Staying Safe Online and Protecting Your Personal Data?