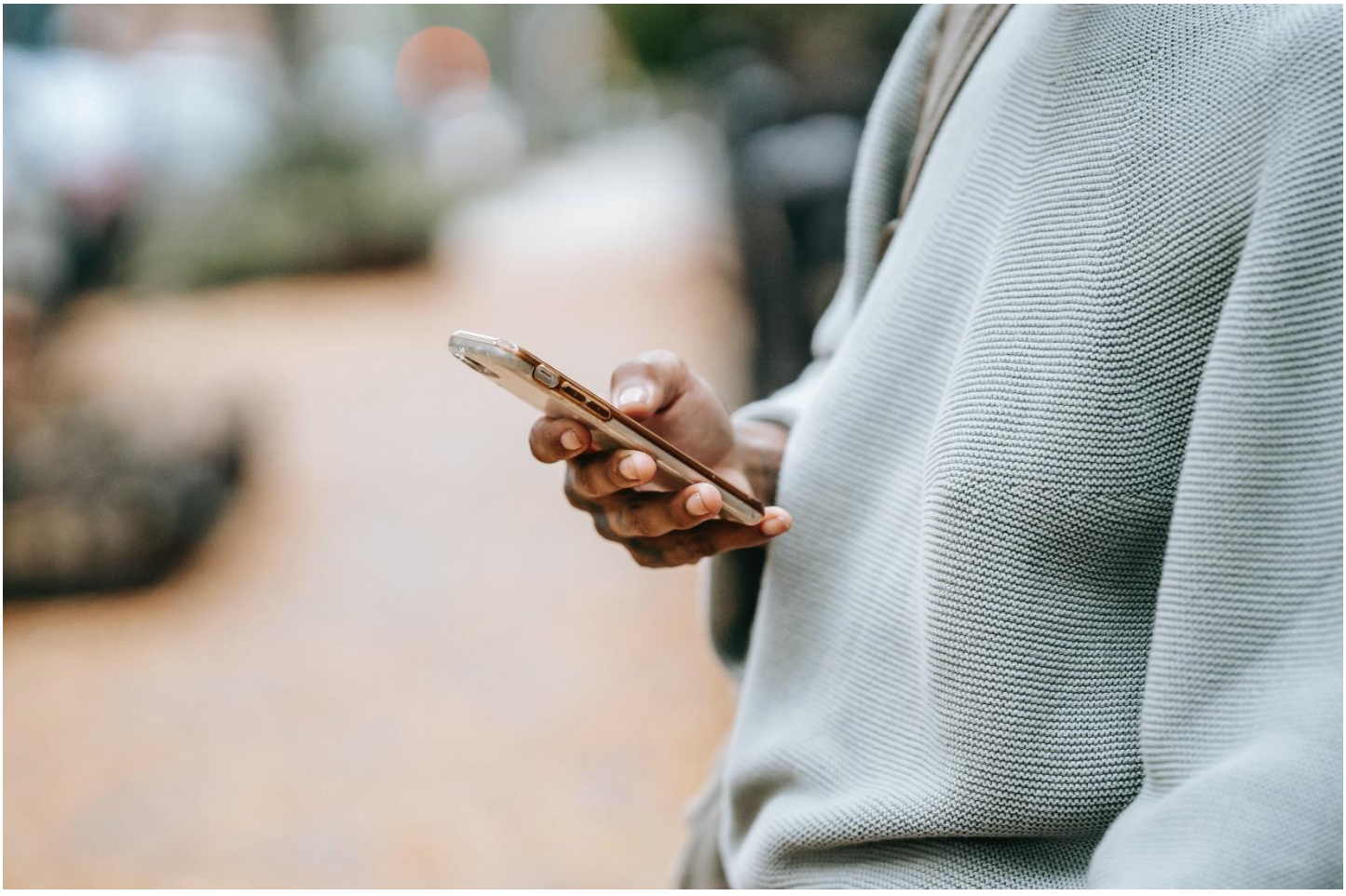
Ohio Attorney General's
Consumer Advocate Newsletter
Keeping Consumers Safe and Informed

October 2022



How to handle scam text messages

Throughout the United States, the Federal Trade Commission says, $131 million was reported lost in 2021 to frauds originating via text messages – a practice known as "smishing." In 6% of the 377,840 total cases, complainants said they lost money, with a median loss of $1,000.

The Federal Communications Commission, which regulates mobile-phone providers, has fielded an increasing number of smishing complaints in recent years – 5,700 in 2019, 14,000 in 2020 and

15,300 last year. The 8,500 complaints it had received through June 30 suggests that the 2022 total could set another annual record.

As regulations aimed at identifying the source of robocalls have tightened, scammers have increasingly turned to texting to wreak their havoc.

Smishing occurs when scammers send a text message that purports to be from a legitimate business or organization. The message might instruct you to click on a link to confirm or input your account information. The text might even falsely claim that you have purchased a product or service costing hundreds of dollars, and it might include a sense of urgency, suggesting that your account will be suspended or that you'll be charged for an item if you don't act immediately. By entering your username and password using the sham link on an impostor webpage, you open the door for a scammer to steal your personal information and gain access to your account.

Smishing scams rely on various prompts to trick their victims. For example, texts might say that an unknown package is ready to be tracked, that your bank is closing your account or denying access to your debit card, that you've won a prize or that you need to confirm the purchase of a product.

Here are some ways to avoid being victimized by scam text messages:

- Check your related accounts first before clicking on a link. If you receive an unusual text or email claiming to be from a trusted business or organization, do not click on the link in the message. Check your accounts through websites or phone numbers that you have verified to make sure your accounts are intact and that you have not purchased any unwanted items. Something to look for: Often a fake link contains a slight misspelling or differs slightly in other ways from the legitimate website.
- Never call back an unknown number. Use the information on the company's official website and not a number listed in an unexpected text.
- Don't pay a stranger with a gift card. If you are asked to pay with a gift card, it's a scam.
- Don't give remote access to someone who contacts you unexpectedly. The contact might claim to be from a government office, computer repair company or popular online store. Remote access to your computer or other electronic devices gives scammers easy access to your personal and financial information, such as your bank account. They might claim to be refunding your money but instead try to steal it.

If you receive an unwanted text message claiming to be from a business, there are four ways to follow up:

- Report it to the Ohio Attorney General's Office at www.OhioProtects.org.
- Report it on the messaging app you use. Look for the option to report junk or spam.
- Forward the message to 7726 (SPAM).
- Report it to the FTC at ReportFraud.ftc.gov.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Seven simple steps to be more secure in cyberspace

In today's world, it's more important than ever to protect yourself in cyberspace. Celebrate Cybersecurity Awareness Month by learning seven simple and practical steps to increase your security online when using smartphones, tablets, notebook computers and other internet-connected devices.

1. **Activate multifactor authentication (MFA) whenever possible.** MFA – available on many of your online accounts, apps and programs – requires you to verify your identity in addition to reciting your password, usually by sending a code to your mobile device. The National Cybersecurity Alliance (NCA) says that, according to Microsoft, "MFA is 99.9 percent effective in preventing breaches." The company says MFA is a must for individuals looking to secure their devices and accounts.

2. **Enable automatic updates.** Ohioans should ensure that their online devices have the latest updates to operating systems, internet browsers and anti-virus programs. Activating automatic updates whenever offered can save you from having to remember to regularly check for updates to these critical programs on your devices. For example, updates on mobile phones may address bugs and security flaws that the operating system has identified.

3. **Use a password manager and regularly change your passwords.** The NCA says that "having unique, long and complex passwords is one of the best ways to immediately boost your cybersecurity." But its own report, conducted with CybSafe, found that only 43% of the public always or very often uses sufficiently strong passwords. Although many people find it difficult to remember their passwords, a reputable and secure password manager can help you perform these tasks. With a password manager, you typically have to remember only your master password.

4. **Use secured Wi-Fi.** Never use free, public Wi-Fi to perform any tasks that require a password or other personal identifying information. This includes online banking, product purchases and other financial transactions. When you do need to enter personal identifying information on a website, be sure the website is secure. How can you tell? Look at the address bar in your internet browser; secure sites typically begin with **https://** (The "s" stands for *secure*). Depending on the browser, the address bar may turn green or show a padlock to indicate that you're doing business on a secure website.

5. **Use firewalls and anti-virus software on all devices.** Your wireless router essentially should act as a basic firewall, which helps keep potential hackers out of your home Wi-Fi network. Ensure that all devices connected to your home Wi-Fi have anti-virus software installed and that it is up to date. The most up-to-date security software, web browsers and operating systems are the best defense against online threats such as viruses and malware, according to the NCA.

6. **Be alert to phishing attempts.** According to the NCA, scammers phishing for personal information make up 80 percent of all cybersecurity incidents. Phishing occurs when someone impersonates a legitimate person, business or organization to try to trick victims into revealing private data, typically by luring them to click on a malicious link that leads to a phony website.

7. **Back up your data.** No one can be certain that home Wi-Fi security is 100% effective, so users need to back up their most important information by either storing it in the "cloud" or copying it onto external hardware, such USB storage sticks or portable hard drives. Information stored with cloud storage services – think Google Drive, Dropbox and Microsoft OneDrive – is maintained on servers accessed over the internet.

For more information about the National Cybersecurity Alliance, visit its website at www.staysafeonline.org. For cybersecurity tips from the Ohio Attorney General's Consumer Protection Section, click here.

Parents and kids: Tips for safer social media and gaming

Ohioans of all ages enjoy belonging to online communities. In recognition of Cybersecurity Awareness Month, we offer tips to help parents and their kids stay safe while on social media and online gaming platforms.

For starters, be sure to review the preceding article on the "Seven simple steps to be more secure in cyberspace." Advice on creating passwords, using multifactor authentication and keeping antivirus software updated is applicable to social media and gaming environments.

In addition, consider these specific tips about online gaming:

- Research any apps before downloading them to make sure they are legitimate and safe. Read reviews and go only to trusted app stores. Note that even in trusted app stores, some apps may not be safe.
- Use a credit card, not a debit card, if you need to enter any payment data for online gaming. Credit cards have additional protections afforded by law.
- Watch out for potentially dangerous links or downloads, especially if they are from a stranger or are unexpectedly provided to you. According to the National Cybersecurity Alliance (NCA), "Cyber criminals will often try to entice gamers into clicking links or downloading malicious files by offering cheats, hacks or other ways to gain an advantage over competitors." One smart tip is to hover your mouse pointer over a link before taking any action. Doing this will reveal the actual URL to which the link will take you.
- Share as little personal information as possible on your public gaming account profile.
- Stay away from online gaming on free, public Wi-Fi to keep strangers from accessing your personal information and digital wallets. If you need to game online while traveling, the NCA suggests considering using a virtual private network (VPN) or hotspot through your cellphone signal to help provide a more secure connection.

- Be aware that parents can configure security and privacy settings for online gaming to limit how much information kids share. Consider parental controls to help institute rules about what your child can do and what they should be restricted from doing while online. This could include whether the child is able to communicate with other gamers, how much time they spend gaming and what – if anything – they are permitted to buy through the gaming environment.

Consider these tips regarding social media platforms:

- Stay current with social media apps your children may be using. Parents should know what their kids are doing online. Be sure to discuss with kids the importance of not interacting with strangers they meet through social media, and make sure they know not to click on any links or download any unknown files. Let your kids know it is OK to talk to you about unsafe interactions with others.
- Recognize that social media posts can live a long life and be distributed beyond a person's intended network of friends. Think before you overshare.
- Make sure your children's privacy settings are as strict as possible, establish guidelines governing their online activities (e.g., length of time online), and consider other parental controls that might be necessary.
- Understand how your personal data is used by social media platforms. According to the Better Business Bureau, "Many sites are designed to collect and sell unauthorized user details and behaviors to advertisers looking to engage in targeted marketing."

For more information about the National Cybersecurity Alliance, visit its website at www.staysafeonline.org. For additional online privacy tips from the Better Business Bureau, click here. For cybersecurity tips from the Ohio Attorney General's Consumer Protection Section, click here.

AG Yost, 32 other attorneys general reach $438 million settlement with JUUL

Attorney General Dave Yost and 32 other attorneys general announced a proposed $438.5 million settlement with JUUL Labs stemming from a two-year multistate investigation into the e-cigarette manufacturer's misguided marketing and sales practices.

"No nicotine marketing to kids! It was wrong when it was Joe Camel, and it's wrong when it's JUUL's 'Miint' and 'Fruut' flavors and their influencer-led targeting," Yost said. "This settlement puts an end to JUUL's trawling for new addicts among our children."

JUUL was, until recently, the dominant player in the vaping market – a position the company attained by willfully appealing to youths in its marketing and advertising, even though its e-cigarettes are both illegal for youths to buy and unhealthy for them to use.

The investigation found that JUUL:

- Relentlessly targeted underage users with launch parties; advertisements using young, trendy-looking models and influencers; social media posts; and free samples. Almost all of JUUL's advertising was conducted on Instagram, Twitter and Facebook. A study of the company's Twitter account found that 45% of its followers were 13 to 17 years old; only 20% were 21 or older.
- Manipulated the chemical composition of its product to make the vapor less harsh on the throats of young and inexperienced users.
- Sold e-cigarettes in youth-friendly flavors, including Miint, Fruut, Bruule, Tobaac, Cool Cucumber, Coco Mint and Mango.
- Falsely implied on its original packaging that the product contained a lower concentration of nicotine than it does; in fact, JUUL contains more nicotine than most other e-cigarettes.
- Suggested in its "Make the Switch" campaign that JUUL was a smoking-cessation device, even though it lacked authorization from the Food & Drug Administration (FDA) to make such a claim.

JUUL has ended its social media marketing and now sells pods only in two flavors: tobacco and menthol.

The settlement will force the company to comply with strict injunctive requirements that severely limit JUUL's marketing and sales practices. Specifically, JUUL has agreed to refrain from:

- Marketing to youths.
- Depicting anyone under age 35 in any marketing.
- Using cartoons in its marketing.
- Paying for product placement.
- Selling brand-name merchandise.
- Selling flavors not approved by the FDA.
- Allowing access to websites without age verification on a landing page.
- Making representations about nicotine not approved by the FDA.
- Making misleading representations about nicotine content.
- Participating in sponsorships or naming-rights deals.
- Advertising in outlets unless 85% of the audience is adult.
- Advertising on billboards, public transportation and in social media (other than testimonials on social media by individuals over the age of 35, with no health claims).
- Using paid influencers.
- Using direct-to-consumer ads unless age-verified.
- Offering free samples.

The investigation was led by Connecticut, Texas and Oregon. Joining Ohio in signing the agreement were Alabama, Arkansas, Delaware, Georgia, Hawaii, Idaho, Indiana, Kansas, Kentucky, Maryland, Maine, Mississippi, Montana, North Dakota, Nebraska, New Hampshire, New Jersey, Nevada, Oklahoma, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Virginia, Vermont, Wisconsin and Wyoming.

As of September 30, 2022, the states were still finalizing and executing the settlement. The proposed $438.5 million would be paid out over six to 10 years, with the amounts paid increasing in proportion

to the amount of time the company takes to make the payments. If JUUL extends the payment period to 10 years, the final settlement could total up to $476.6 million.

Both the financial and injunctive terms exceed any previous agreement that JUUL has reached with other non-participating states to date.

Unrelated to this settlement, the FDA on June 23, 2022, ordered JUUL to stop selling its products in the United States. Following an appeal by JUUL, however, the FDA has since decided to let JUUL's products stay on the market temporarily while the agency conducts an additional review.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.