October 2023

SecurityAwarenessNews

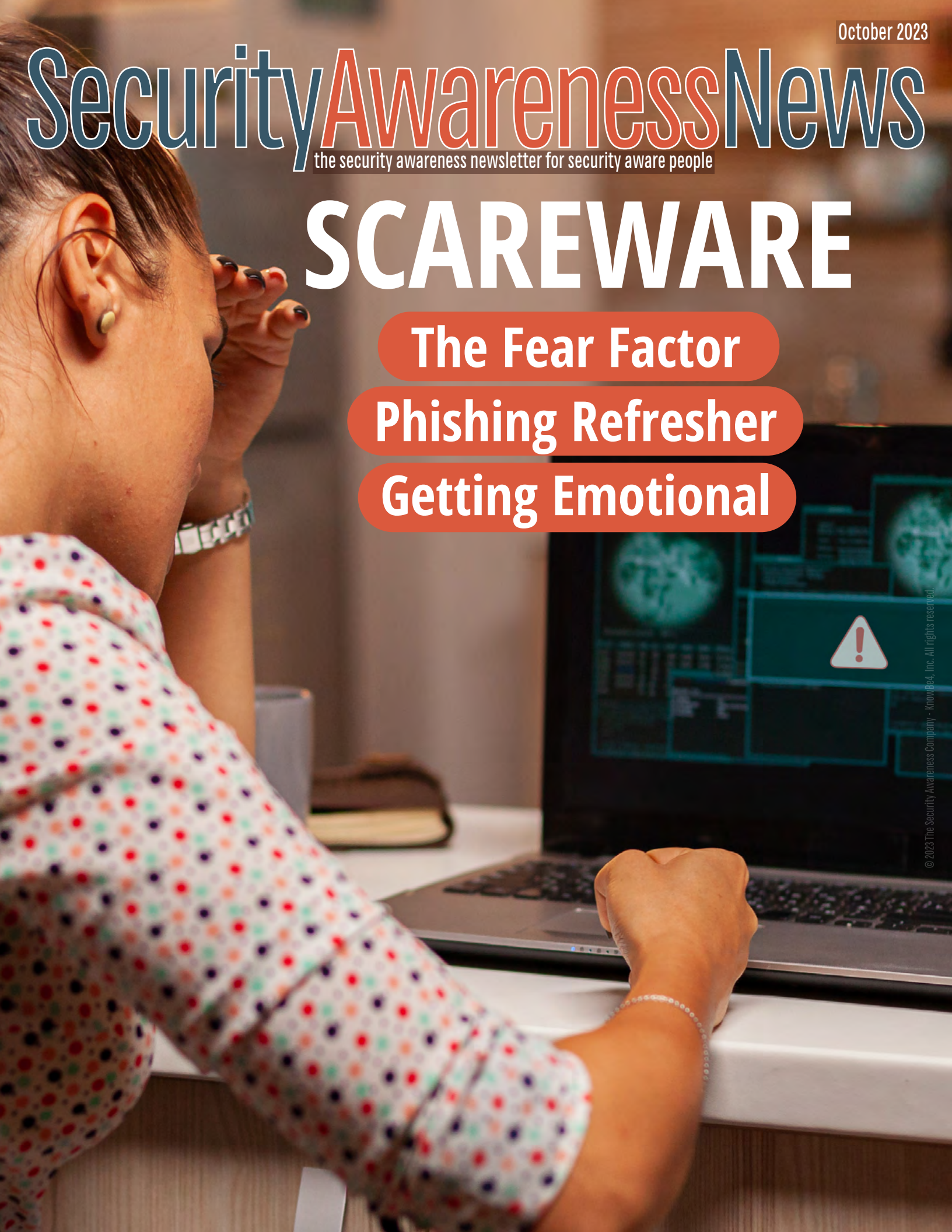
the security awareness newsletter for security aware people

SCAREWARE

The Fear Factor

Phishing Refresher

Getting Emotional



THE FEAR FACTOR

This is an example of scareware: a malicious pop-up advertisement that can appear even on legitimate, trustworthy websites. Here's what can happen if someone falls for it by clicking:

They download malicious software (malware)

Malware comes in many forms and is used for different purposes. It can steal personal information, spy on people's internet activities, and generally cause devices to lose functionality.

They lose money

As with many online scams, the attackers are trying to get paid. Scareware convinces people they need to buy security software that doesn't actually work to fix a problem that doesn't exist.

They end up on a malicious website

Similar to downloading malware, a malicious website could infect devices or might prompt the visitor to enter their personal information, such as passwords, bank numbers, and national ID numbers.

Avoiding Scareware

Like many online scams, scareware works by stoking fear. When people encounter situations that make them feel alarmed or anxious, they are often quick to react. Leveraging the fear factor is one of the best ways to influence that reaction and cause someone to make a poor decision.

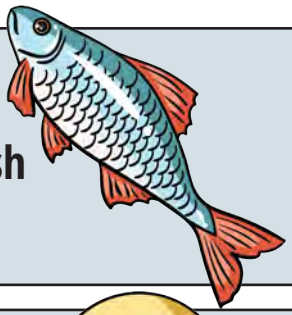
In fact, the strategy behind scareware is similar to other phishing attacks — the use of deception to mislead people into doing something against their best interest. You can avoid it by staying alert, slowing down, and thinking before clicking or taking action.

In other words, don't let your emotions guide you when it comes to cybersecurity. Instead, let logic take control and use situational awareness. Here at work, if you encounter scareware or any other unusual activity, report it immediately!

PHISHING REFRESHER

Phishing attacks are one of the biggest threats facing individuals and organizations alike. Let's open the tacklebox of fishing cliches and review how these scammers attempt to lure people in.

The Phish



Anyone can be a target. In fact, phishing is perhaps the most common scam around and the one you're most likely to encounter. While many attacks cast a wide net with generic messages, others are much more advanced. Like any good angler, an advanced attacker will know what they're trying to catch by targeting specific people or organizations.

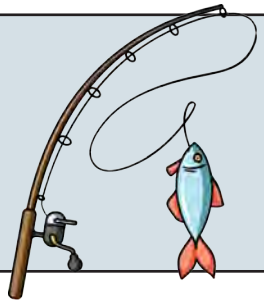
The Bait

If you want someone to bite, you must use the right bait. It's all about temptation. A phishing email, for example, needs to have an intriguing subject line that increases the likelihood the recipient will open it. That's why many attacks use attention-grabbing subjects like "Alert! Your account has been suspended!"

The Hook

The bait you use is only as good as the hook it's threaded on. A good hook helps ensure that when someone bites, they'll actually stay on the line and get reeled in. Therefore, it's vital that the message or story — the hook — gains someone's trust or tricks them into making a bad decision, like opening a malicious link or attachment.

The Catch



There's no catch-and-release with phishing attacks. Once someone falls for the scam, they could have their personal information stolen or have their device infected with malicious software (malware). No matter the case, falling for a phishing scam can lead to personal and professional harm.

Blue marlin are one of the ocean's most majestic fish. According to many fishing experts, blue marlins are also one of the most difficult fish to catch. They require robust strategies, skilled timing, and hours of endurance to reel in if you're fortunate enough to hook one.

So be the Blue Marlin. Make life difficult for the many phishers of the world by:

- Staying alert for common warning signs, such as threatening or urgent language
- Carefully reviewing messages before taking an action
- Following organizational security policies
- Reporting suspected phishing attacks immediately

the security awareness™ COMPANY
a KnowBe4 company

Getting Emotional:

How Scammers Influence People

Critical thinking and common sense are perhaps the most vital mental processes that help people avoid scams. Unfortunately, those processes are not infallible. Cybercriminals know how to circumvent them by manipulating human emotions, such as these:

FEAR

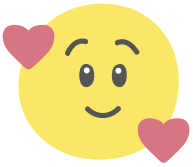
Scareware (malicious pop-ups) isn't the only way scammers leverage the fear factor. Phishing attacks notoriously feature threatening language designed to trigger emotional responses. One typical example is the "Payment Overdue" message that claims you have an outstanding balance. The email will contain a malicious attachment disguised as an invoice.

SYMPATHY

When playing the sympathy card, scammers hope the target will feel bad for whatever scenario they dream up. A sick relative, unexpected bills, an injured pet — anything that might trick someone into sending money. This common attack works best when the scammer impersonates a family member or a friend who's allegedly in a desperate situation.

CURIOSITY

Many cybercriminals know that intrigue leads to action. That's why they leave malicious USB flash drives or charging cables in public areas. All it takes is one curious person to find the drive or cable and plug it into their device, which can then infect that device with malware.



LOVE

Dating sites and apps make lovely matches for criminals who use romance scams to steal money. It's a longplay where they establish a romantic relationship with someone. After several weeks of building the relationship, the scammer then creates a sob story and asks their new companion for financial help.

EXCITEMENT

Imagine receiving an email that states, "Congratulations! You've won an all-expenses-paid trip!" Sounds wonderful, right? Of course, to claim the prize, you must first provide your full name, home address, phone number, and date of birth. This is a common data-stealing technique.

Don't let these tactics of emotional manipulation influence you. Treat any request for confidential data or money with a high degree of skepticism. Follow your instincts and use situational awareness. When in doubt, don't respond, don't click, and don't make assumptions.

the security awareness™ COMPANY
a KnowBe4 company