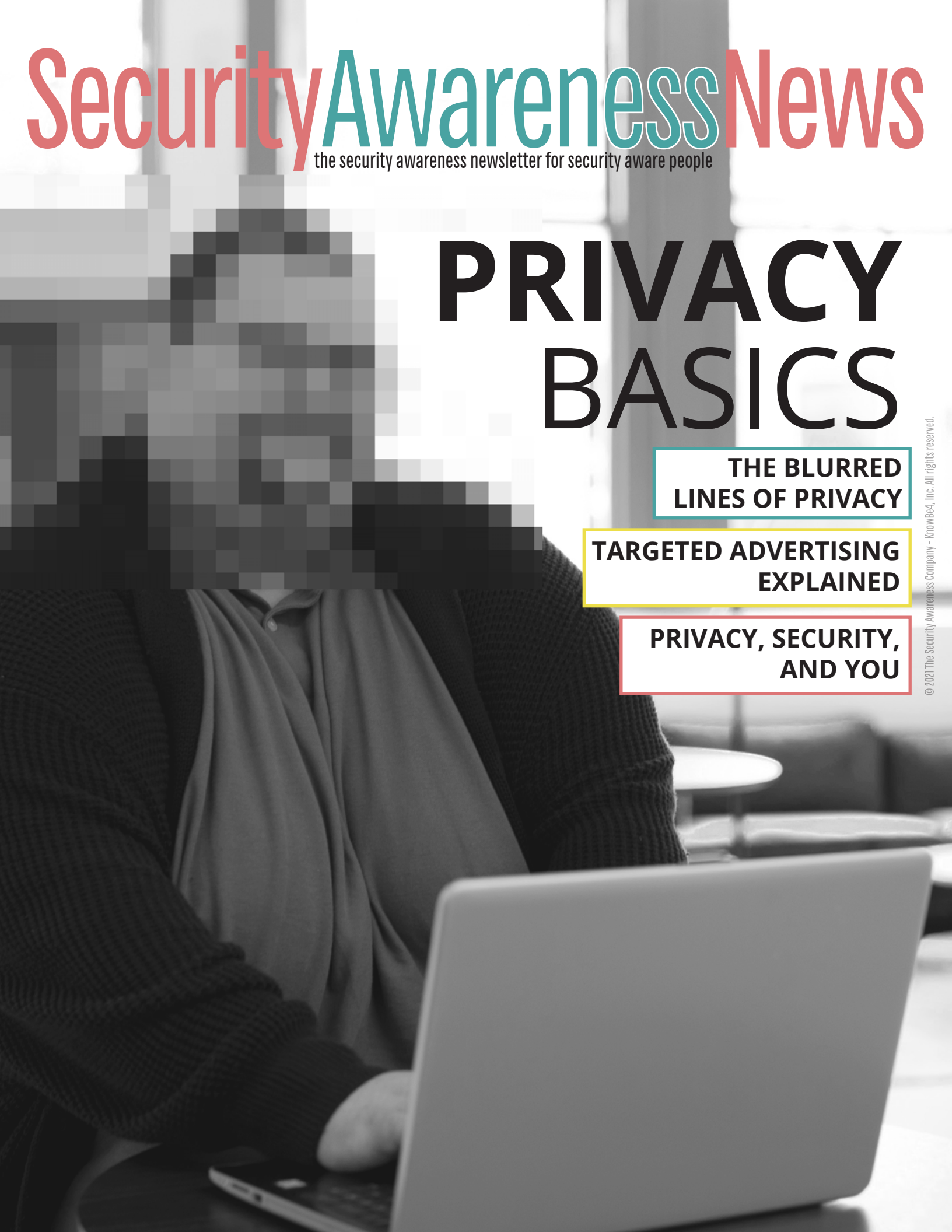
SecurityAwarenessNews

the security awareness newsletter for security aware people



PRIVACY BASICS

THE BLURRED LINES OF PRIVACY

TARGETED ADVERTISING EXPLAINED

PRIVACY, SECURITY, AND YOU

THE BLURRED LINES OF PRIVACY

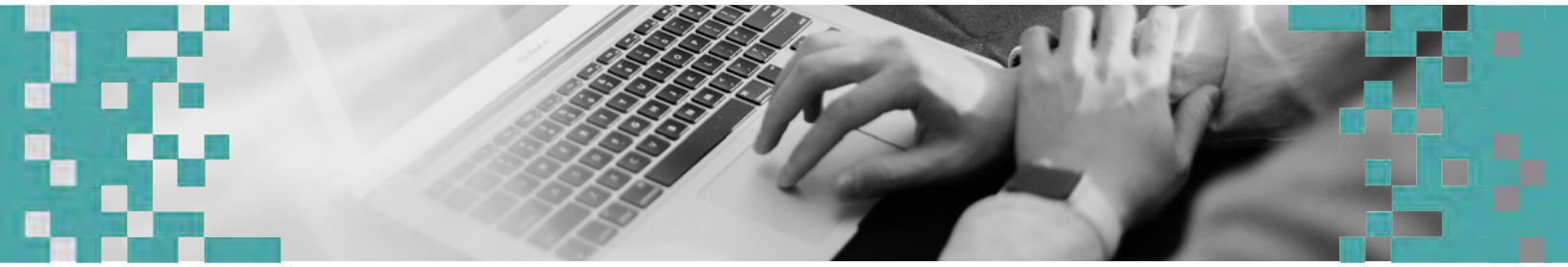
"Privacy means people know what they're signing up for..." – Steve Jobs

It's no secret that websites, mobile applications, and online services collect endless amounts of data from billions of people. The question becomes: Can privacy truly exist in a world where nearly everything we do online gets tracked, stored, and sometimes sold to third-parties?

The answer to that question remains the focus of privacy advocates, who have long voiced their concerns regarding the ongoing collection of personal information.

In many cases, their worries are valid. Personal data has become a currency that provides access and convenience. Convenience, of course, usually comes at a cost. In terms of data collection, that cost isn't always made obvious, which is exactly what Steve Jobs was referring to when he said "Privacy means people know what they're signing up for."

Many people are unaware of what they're consenting to when they use online services or download applications. And when you think about how difficult it is to trace who has access to which data, you can quickly see how the line between privacy and convenience blurs.



Here at work, however, the answer to data privacy couldn't be clearer. When our organization collects personal information—which includes anything that can be used to identify specific individuals—it's our responsibility to protect that information. That's why we need all employees to:

- Stay alert for phishing attacks and other scams
- Always follow organizational security policies
- Report all security incidents immediately
- Protect access, both digital and physical

Committing to that short list of action items helps maintain the privacy of anyone who has entrusted us with their information. Even though data collection cannot be avoided in the modern work environment, data leaks can be avoided. But only if we all do our part.
Have questions or need more information about your role? Please don't hesitate to ask!

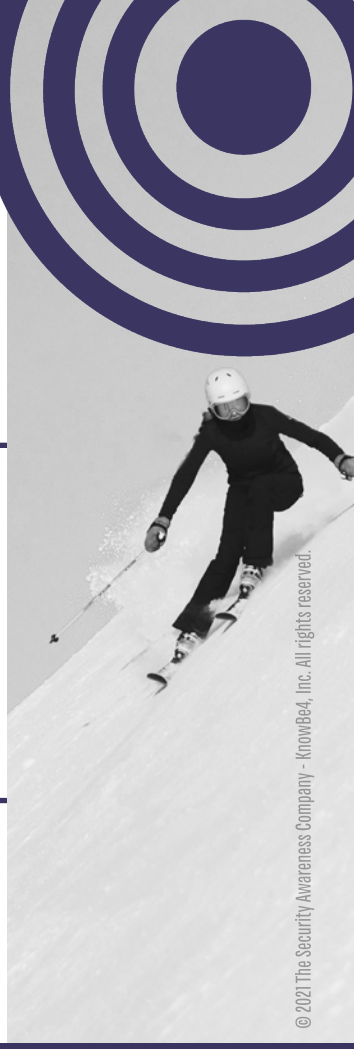
TARGETED ADVERTISING EXPLAINED

Take a moment to consider the multitude of free services available online: maps, spreadsheets, documents, email, photo storage, and many more. Unfortunately, nothing is ever actually free. Those services are provided in exchange for personal information such as browsing habits, interests, age, and location. That data can then be used to deliver targeted advertisements that suggest relevant products while you browse websites.

For example, a 32-year-old person living in Lake Tahoe, California who frequently visits a ski resort is likely to see advertisements for snowboards. Marketers (in theory) don't know specifically who that person is, but if that person has location services enabled on their phone and they use any of the free services from above, marketers likely know that the individual:

- Is young and possibly in good shape (especially if they ever visit a gym)
- Lives in an area that's a hotspot for winter sports
- Visits ski resorts (based on location services or check-ins)

That's a simplified example, but it demonstrates how marketers use data collection to push products. You've likely experienced this yourself, especially on social media where advertisements sometimes feel intrusive. (If you're interested in learning why you see advertisements so quickly, do some research on a technology called real-time bidding.)



Unfortunately, it's nearly impossible to avoid targeted advertisements, but you can improve your overall online privacy with a few simple actions:

SWITCH TO AN ALTERNATIVE BROWSER

Most people use a mainstream web browser to access the internet. While those browsers offer the most features, they also collect the most personal data. Switching to an alternative browser (or search engine) that is focused on privacy can help reduce data collection.

USE A VPN

A virtual private network (VPN) encrypts your internet traffic, which not only offers anonymity, it also adds a vital layer of security. Always use a VPN when connecting to a public network and consider using one at home to hide your location and browsing activity.

INSTALL PRIVACY EXTENSIONS

There are several browser extensions geared towards privacy that prevent websites from tracking or monitoring your web activity. They also eliminate pop-ups, which can help you avoid potentially malicious advertisements (known as malvertising).

As a reminder, never install any applications or extensions on work-issued devices without permission!

PRIVACY, SECURITY, AND YOU

When we collect confidential data, as most organizations do, we enter an agreement of trust. It's our responsibility to protect data and never use it for any reason beyond what was initially agreed upon. That's the simplified definition of privacy.

Security is how we maintain privacy. It's a combination of technology—such as firewalls and threat monitoring software—and human efforts, like using common sense and following policy. At the intersection of privacy and security is you: the last line of defense. You, and all members of our organization, ultimately determine whether or not we honor the agreement of trust. With that in mind, let's review a few quick examples of how you can help maintain both privacy and security.

MAINTAIN PRIVACY BY:

Never sharing sensitive information on public forums, especially social media where cybercriminals are on a constant hunt for data.

Minding your surroundings when working remotely. Make sure no one can hear your conversations, see your screen, or access anything work-related.

Respecting the access granted to you. Never share your passwords or keycard/ badge with anyone else. Always properly dispose of sensitive materials when no longer needed.

MAINTAIN SECURITY BY:

Utilizing strong passwords. A strong password is at least 12 characters long, unique to every account, and never written down or stored in a manner that threatens security.

Staying alert for phishing attacks. Carefully inspect all messages for warning signs like bad grammar and threatening language. Think before you click on any links or attachments.

Always following policy. There might be no simpler measure of security than following security policies, which were designed to ensure that confidential information remains confidential.

If you think these examples seem obvious or redundant, you're not mistaken. In fact, arriving at that conclusion illustrates an important point: Maintaining security (and by extension, privacy) isn't always a complex process. Most of the time, it requires nothing more than a little common sense and situational awareness.