SecurityAwarenessNews

the security awareness newsletter for security aware people

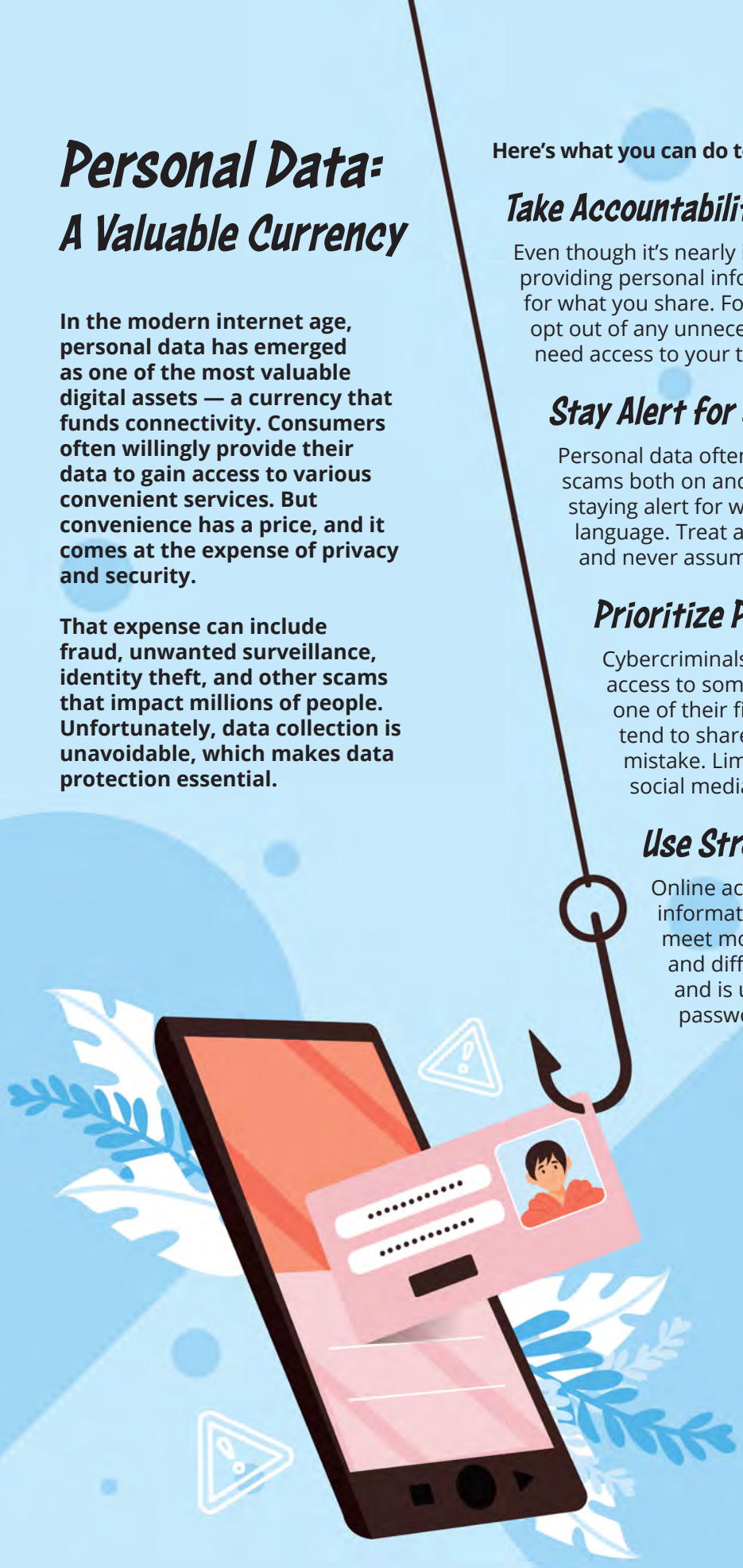
The Price of Convenience

- Personal Data: A Valuable Currency
- Mobile App Security
- Data Privacy, Compliance, and Policy

Personal Data:
A Valuable Currency

In the modern internet age, personal data has emerged as one of the most valuable digital assets — a currency that funds connectivity. Consumers often willingly provide their data to gain access to various convenient services. But convenience has a price, and it comes at the expense of privacy and security.

That expense can include fraud, unwanted surveillance, identity theft, and other scams that impact millions of people. Unfortunately, data collection is unavoidable, which makes data protection essential.



Here's what you can do to keep the cost of privacy and security down:

Take Accountability

Even though it's nearly impossible to use various services without providing personal information, it's important to take accountability for what you share. For example, when using mobile applications, opt out of any unnecessary permissions; a flashlight app shouldn't need access to your text messages.

Stay Alert for Scams

Personal data often gets stolen when people fall for common scams both on and off of the internet. You can avoid this by staying alert for warning signs, such as threatening or urgent language. Treat all requests for information with skepticism and never assume someone is who they claim to be.

Prioritize Privacy

Cybercriminals are always looking for easy ways to gain access to someone's personal information. Social media is one of their first stops because they know some people tend to share more than they should. Don't make that mistake. Limit what information you make public and set social media accounts to private.

Use Strong Passwords

Online accounts often have access to highly confidential information. Protect them with strong passwords that meet modern standards. A strong password is long and difficult to guess, avoids repeated characters, and is unique to each account. At work, ensure your passwords adhere to organizational policy.

Remember:

Security awareness is vital to protecting personal data, both at work and at home.

Mobile App Security

Smartphone applications harness an amazing combination of connectivity and convenience. That combination also makes them a top target for cybercriminals who view apps as opportunities. Protect the computer in your pocket by adhering to these app security essentials:

Research Developers

There is an app for almost everything, including cybercrime. Attackers have been known to create apps that are designed to steal information or money. As a general rule, only download apps from legitimate sources and reputable developers. Avoid apps that only have a few downloads and reviews.

Stay Updated

Out-of-date software can present unnecessary security risks. You can avoid those risks by keeping your phone and apps up to date. Consider enabling automatic updates so you never miss a crucial security fix.

Review Permissions

Many apps will ask you to allow various permissions, such as location services and access to text messages or photos. These permissions are often needed for the app to function properly. Even so, it's important to review what an app is requesting and only allow the minimum permissions necessary.

Remove Unused Apps

People tend to install several apps over time and then forget about them. This can lead to privacy issues because those apps might be collecting personal data even though they aren't being used. Make it a routine to occasionally review and uninstall software you no longer need.

Remember:

For work-issued devices, always follow policy regarding which apps you're allowed to install and when updates should be implemented.

Data Privacy, Compliance, and Policy

It's no secret that organizations around the world collect and analyze personal information. It's also no secret that the data usage practices of some organizations ushered in concerns about privacy, shining a focus on several key questions:

What data was collected?

Who has access to it?

Is it being used for legitimate purposes?

How is it being protected?

Enter data privacy regulations, many of which require organizations to answer those questions. There are now several compliance standards worldwide sharing a common goal: increase the data privacy rights of individuals.

The General Data Protection Regulation (GDPR) is one of the most notable examples. It specifies the rights of individuals located in the European Union and gives people expanded control over their personal information. As examples, the GDPR grants individuals the right to:

- ***Have data corrected or erased***
- ***Know what data is being used and why***
- ***Object to, or opt out of, data collection***

The GDPR set the global stage for data privacy legislation, and Europe has since been joined by several other countries that have adopted similar laws. Those laws generally require organizations to develop their own data protection standards internally and remain transparent about data usage.

What does all of this mean for you? Obviously, you're not required to be an expert on compliance laws. You are, however, required to always follow organizational policies.

Policies are created for several reasons, and the key among them is ensuring an organization can adhere to any applicable compliance requirements. Note that compliance is about more than laws and regulations. It's about people and their right to data privacy. Policies exist to ensure those rights are upheld.

Therefore, by always following policy, you help maintain the privacy and security of people, not just data.

Remember:

You are the last line of defense when it comes to protecting confidential information.