January 2023

# SecurityAwarenessNews

the security awareness newsletter for security aware people

# Data Privacy Fundamentals

## Data Protection Refresher

## Digital Health Checkup

## The Future of Data Protection

# Data Protection Refresher

At the center of information security exists an ongoing effort to protect confidential information. Cybercriminals are constantly on the offensive, using a variety of tactics in hopes of stealing data and, by extension, money. Here's a quick refresher of what's at stake, how it's vulnerable, and what you can do to ensure the privacy and security of information.

## THE TYPE OF DATA AT STAKE

On a personal level, home addresses, full names, birthdates, banking numbers, and national ID numbers all represent just a few examples of data that cybercriminals seek out. They also seek confidential corporate information such as business strategies, top-secret recipes or blueprints, employee directories, and more.

## HOW DATA GETS STOLEN

In some cases, data theft involves highly sophisticated cyberattacks. In most cases, however, criminals use social engineering — emotional manipulation tactics designed to mislead people into doing something they shouldn't. Human error, such as misconfiguring network settings, accidentally leaking information, and using weak passwords, are also common contributors to data theft.

## YOUR ROLE IN PROTECTING DATA

Whenever you're granted access to sensitive information, you become responsible for its privacy and security. While data protection involves many factors, here's a quick rundown of the fundamentals:

Always follow policy. Organizational policies exist, in part, to ensure that confidential information remains confidential.

---

Use strong, unique passwords. The longer the password, the harder it is to crack. Make sure every account gets its own unique password.

---

Avoid assumptions. You can prevent social engineering attacks by not assuming someone is who they claim and by using situational awareness.

---

Learn the warning signs. Phishing attacks can be identified by common signs like bad grammar, urgent or threatening language, and random links or attachments.

---

Ask questions. If you need clarification on anything, or are simply curious to learn more about protecting data, please ask!

---

Report security incidents immediately. If you see something, say something. The longer an incident goes unreported, the more harm it could cause.

# Digital Health Checkup

It's likely that at this very moment, some entity somewhere is collecting and storing your personal information. Even though data collectors are subject to multiple laws that are designed to protect your privacy, you can still take matters into your own hands. Here's a quick questionnaire to help you maintain your digital well-being.

## Have you reviewed privacy settings for social media accounts?

Social media platforms have a long history of questionable data-collection practices. You can control certain aspects of your privacy by taking the following actions:

- ☐ Disable location tracking services
- ☐ Remove permissions from all apps, games, websites, and business pages
- ☐ Don't allow the platform to connect to other apps or services
- ☐ Set your profile to private and only friend people you know and trust

## Do you know how to spot common online scams?

Train yourself to identify when you're being targeted by staying alert, thinking before you click, and treating all requests for information or money with skepticism. Here are a few common online scams to watch out for:

- ☐ The one where a pop up claims your computer has been infected
- ☐ The one where you're offered a large sum of money for an upfront payment
- ☐ The one where a service or entity asks for payment via gift cards
- ☐ The one where an email claims an account has been disabled due to fraudulent activity

## Did you allow mobile applications to have extended permissions?

Not only do scammers create malicious applications and upload them to popular app stores, many legitimate applications tend to collect excessive amounts of personal data. Always question why an app needs:

- ☐ Access to your camera or microphone
- ☐ Access to your contacts
- ☐ Access to your location
- ☐ Access to your text messages

Generally speaking, if the permissions granted to the app are not necessary for functionality (especially if it's a function you don't intend to use), block them.

# The Future of Data Protection

Accurately predicting the future requires an ability to build complex projection models based on previous trends. Where data protection is concerned, no such models are necessary, as it's reasonable to assume two things will remain true for many years to come.

## The future will include aggressive and ongoing personal data collection.

It's hard to imagine data collection becoming even more pervasive than current day. Past trends, however, suggest otherwise. As technologies and services evolve, they become increasingly reliant on end-user data to function properly.

Case in point: virtual reality (VR). In the near future, avatars — the digital version of users — will almost perfectly mirror how people look, walk, and jump. The technology effectively scans entire physical beings into a digital environment, which is a massive amount of data that needs to be stored somewhere, by someone (hint: that someone will not be the consumer). As technologies like VR become more prevalent, so too will their database of end-user behaviors and metrics.

## The future will not include a 100% guarantee of the security of that data.

Over the last several years, security solutions have become smarter and more effective. Many developers now implement automated systems like artificial intelligence (advanced computers) and machine learning (systems that learn from data and evolve accordingly).

The idea behind both is to detect and respond to threats faster than humans.

Unfortunately, even as security technologies improve, two vital factors work against them.

1. Technology can and will fail
2. Cybercriminals also evolve and will leverage advanced technologies

Those factors highlight a key concept: You are the future of data protection. Technology might help, but it will always fall behind criminal tactics, which are designed to remove technology from the equation (such as social engineering).

As always, security and privacy will ultimately be determined by the individuals who stay alert, identify threats, and report them immediately.