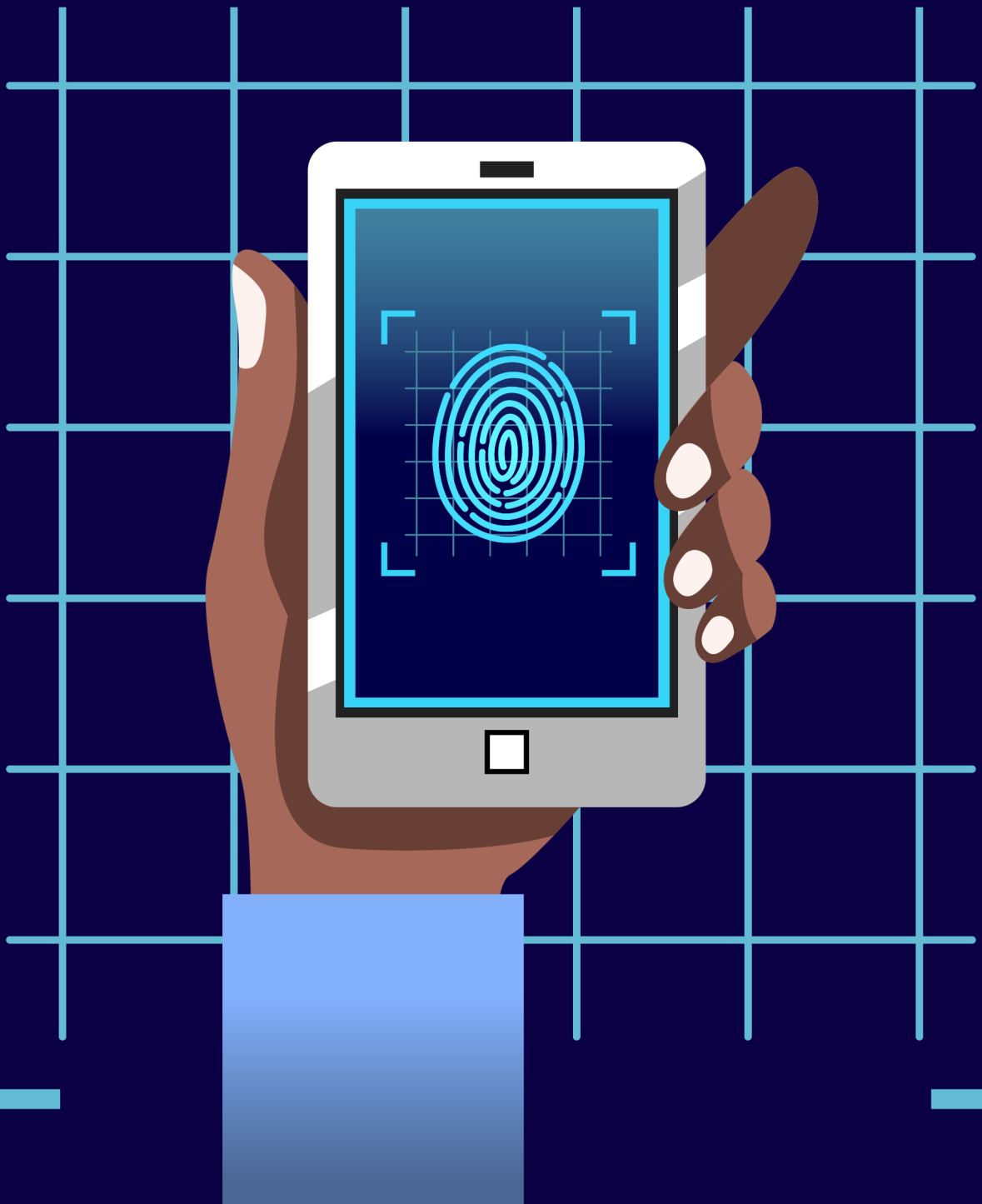
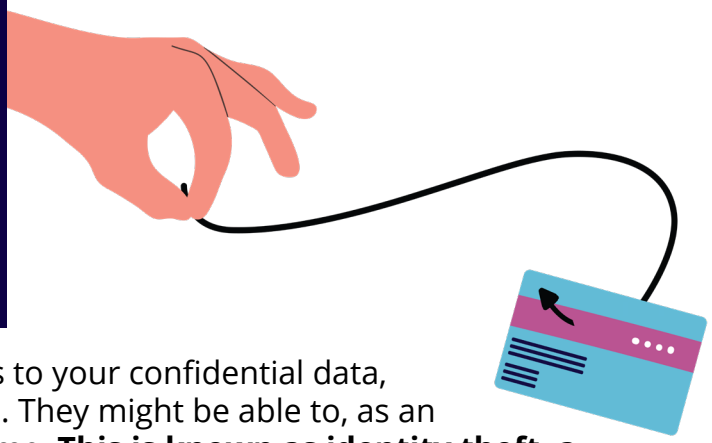
SecurityAwarenessNews

the security awareness newsletter for security aware people

Protecting Your Digital Identity



Avoiding Identity Theft



Imagine what a criminal could do if they gained access to your confidential data, such as your full name, national ID number, and more. They might be able to, as an example, open accounts or apply for credit in your name. **This is known as identity theft, a common scam that involves using stolen or leaked information to commit fraud against people.**

The key to avoiding identity theft is understanding how cybercriminals attempt to steal data in the first place. Let's review the most common ways this occurs.

Phishing Emails

Phishing is an attack that attempts to lure people into making security mistakes, such as opening malicious links or attachments, and revealing confidential information. These attacks are prevalent in cybersecurity, but can be recognized through common warning signs, such as threatening language, urgent requests, and unrealistic promises.

Suspicious Phone Calls

Similar to phishing emails, scammers will call you and pretend to be someone else. For example, they might claim to be from a bill collection agency and state that you have an overdue account. As a general rule, never provide payment or personal information to a random caller.

Malicious Text Messages

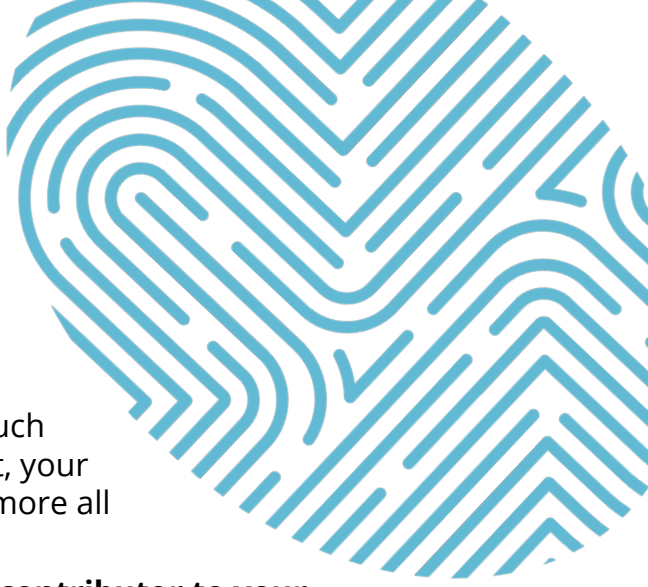
Malicious text messages use the same tactics as most phishing attacks, where the scammer pushes a sense of urgency. They will often include a link that might direct you to a malicious website or instruct you to download a malicious application. Never click on these links.

In all cases, your number one defense is skepticism. If you're ever asked to provide highly confidential information, stop and think. Who is asking? Why do they need this information? Is anything about this situation unusual or unexpected?

Keep in mind that legitimate entities and organizations will never randomly ask you to provide confidential data. For example, a bank won't suddenly call you and request that you confirm your account numbers or passwords. This is true through all forms of communication.

So stay alert, and when in doubt, reach out to whoever is asking for your information through trusted methods, such as their legitimate phone number or website.

Managing Your Digital Footprint



If you've ever encountered an advertisement for something you recently searched for or interacted with, it's because much of what you do online can be tracked. The websites you visit, your search history, social media activity, online purchases, and more all form what is known as your digital footprint.

It tells the story of your internet activity and is a major contributor to your online reputation.

Why Your Digital Footprint Matters

The concept of a digital footprint is important because:

- It is often permanent and difficult to erase or control once it's online
- Some of it may be public, including what you post or share on social media
- It shapes your online reputation, which can be just as important as your offline reputation

It can also be used by cybercriminals with malicious intentions. For example, an attacker can scan social media profiles to find details about someone and use those details for personalized scams.

Managing Your Digital Footprint

While it's nearly impossible to avoid digital footprints, you can manage them by taking a proactive mindset. Here are three ways to do that.

Share Less
Some people tend to overshare personal details, especially on social media. It's best to limit what you publicize, remain selective about who may access what you share, and ensure only people you know and trust can view your full profile. Never post anything confidential.

Use Discretion
Always use discretion when posting anything online. Parts of your digital footprint are public and might be accessed by potential or current employers and other entities. Posting anything offensive or hateful can harm your reputation.

Take Advantage of Privacy Settings
Most web browsers provide a variety of privacy settings you can customize. Take advantage of those settings to control what's being tracked or made publicly available. For example, some browsers allow you to control location information, what data gets saved and for how long, and whether to retain your search history.

Four Tools That Enhance Personal Security

Security is a blend of staying aware of various threats and using technology to assist you in avoiding those threats. Here are four tools that can do just that.

Password Manager

A password manager is software designed to store and manage your login credentials for various websites and services. It allows you to create and use long, complex, and unique passwords for every account without the need to memorize them. You only need to remember one strong master password to unlock the application.

Multi-Factor Authentication

Multi-Factor Authentication, or MFA, provides an additional layer of security for your online accounts. After entering your password, a service will require additional authentication methods before allowing access to your account. This crucial process protects your information even if someone manages to steal your password. It's best to enable MFA wherever it's available.

Account Security Lock

Depending on which services you use, you might be able to place a security lock on your accounts. This free service restricts access to your financial records and personal information. When activated, the lock prevents new financial service providers from viewing your history, which helps protect against identity theft and unauthorized accounts being opened in your name. You must contact each institution individually to implement this protection.

Automatic Updates

Outdated software and firmware are often the source of security vulnerabilities. Cybercriminals actively scan for these weaknesses to gain unauthorized access to systems, which can lead to theft of confidential information or allow them to spread malicious software. To avoid this, always keep your software and devices updated to the latest versions. In some cases, you can enable automatic updates so you never miss critical security patches.

Reminder: At work, always follow policies and never install any software or applications unless they've been explicitly approved.

knowbe4