THE DATA DANGER ZONE

What happens to your information—and how to keep it safe

THIS MONTH'S TOPICS:

Personal data is constantly being collected, shared, and targeted—often without people realizing how frequently it happens or who has access to it. In this month's newsletter, we break down how personal information enters the data marketplace, what happens when that data is exposed in a breach, and why these incidents matter to individuals and organizations alike.

You'll also find clear, actionable tips for safeguarding sensitive information, along with a spotlight on Advanced Persistent Threat (APT) Attacks, so you can recognize red flags before they lead to real-world consequences.

YOUR DATA FOR SALE HOW DATA BROKERS GET PERSONAL INFORMATION

IMAGINE THIS:

You wake up. Check your phone. Check Email. Scroll social media. Order coffee. Google a random question. Click a website link. By lunch, you've created hundreds of data points. And here's the twist: You're not the customer. **You're the product.**

WELCOME TO THE DATA MARKETPLACE

There's an entire industry built around collecting, packaging, and selling personal information. These companies are called **Data Brokers**. They gather their data from:

- **Public records** - You buy a house, and your name and mortgage is scraped
- **Social media** - You post about your vacation, brokers log travel dates, family photos
- **Online purchases** - Retailers track what you buy and how often you shop
- **App usage** - A weather app sells location history, where you spend your time, etc.
- **Loyalty program** - Reward cards track purchases
- **Location data** - Your phone pings cell towers and collects GPS data
- **Website Cookies** - Track browsing behavior across websites.

DATA BROKERS BUILD A PERSONAL PROFILE

Specific to you, and not just with your name and email. They can estimate:

- **Income level**
- **Political views**
- **Health conditions**
- **Shopping habits**
- **Family size**
- **Debt likelihood**

And yes—**this data gets sold.** Advertisers want precision. Political campaigns want influence. Scammers want vulnerability. Data brokers don't usually sell to criminals directly, but once data exists and spreads across platforms, breaches and misuse become inevitable.

Lifecycle of a Data Breach

What Happens: Before, During, and After

Phase 1: Before the Breach

Breaches usually begin long before anyone even notices. Common entry points include phishing emails, weak passwords, spoofed websites, malware, unpatched software, and more. Data can slip in a seemingly unlimited amount of ways.

Phase 2: During the Breach

Once they've found a way in, attackers move across systems to identify high-value data. They can disable security tools and software protection to ensure they go untraced. They can extract data in small, unnoticeable ways, leaving the victim in the dark.

Phase 3: Discovery

Breaches are typically discovered in one of three ways.

1. Internal security detects unusual activity
2. A third party reports stolen data
3. The attacker announces it.

Sometimes breaches aren't discovered for 200+ days, giving attackers ample time to extract sensitive info. The longer a breach is undiscovered, the greater the financial, operational, and reputational damage tends to be.

Phase 4: Aftermath

Once a breach is discovered, the real fallout begins.
Organizations must notify affected customers, report the incident to regulators, and brace for legal scrutiny. This all takes place while absorbing financial losses, repairing reputational damage, and fighting to regain customer trust.

But the impact doesn't stop at the corporate level. For individuals, the consequences can be deeply personal and long-lasting, including identity theft, fraudulent credit activity, medical identity theft, tax fraud, and highly targeted social engineering attacks. Unlike the breach itself, which may last weeks or months, the ripple effects can follow victims for years.

SCAM OF THE MONTH: APT ATTACKS (ADVANCED PERSISTENT THREAT)

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

An employee at a mid-sized organization received what appeared to be a routine email from a trusted software vendor. The message referenced an ongoing project, used familiar language, and included a link to review "updated documentation." Everything looked legitimate, so the employee clicked the link and signed in using their work credentials. Unbeknownst to them, the site was a convincing fake designed to capture login information.

Over the following weeks, attackers quietly used those stolen credentials to access internal systems, monitor communications, and move laterally through the network. Because there were no immediate disruptions, the activity went unnoticed. By the time unusual behavior was detected, sensitive data had already been accessed and exfiltrated. This slow, deliberate approach is a hallmark of an Advanced Persistent Threat (APT), where attackers focus on long-term access rather than quick wins.

DID YOU SPOT THE RED FLAGS?

- The link in the message led to a login page that looked familiar but wasn't hosted on the vendor's official domain
- The message created a sense of routine ("updated documentation") without a clear reason or deadline.

HOW TO PROTECT YOURSELF

- Verify unexpected emails and links—even if they appear to come from trusted vendors or contacts.
- Use multi-factor authentication (MFA) to prevent stolen credentials from being enough to gain access.

PRACTICAL STEPS TO SAFEGUARD SENSITIVE INFORMATION

Let's shift from fear to control: **You just need the right habits.**

Use Strong, Unique Passwords

- Never reuse passwords
- Use complex passwords
- Use a password manager
- Aim for 12+ characters minimum

Turn On MFA

If your password is a lock, MFA is a deadbolt. Even if attackers get your password, they still need the second factor to get in. This one step blocks the majority of automated attacks.

Think Before You Click

STOP. Pause. Hover over links. Check sender addresses carefully. Look for subtle misspellings and anything that feels off. Be skeptical of urgency. Slowing down is your superpower.

Keep Software Updated

Delaying updates leaves vulnerable software. These leave you out of the loop when engineers fix critical bugs. Always enable automatic updates so your software is as safe as possible.

Protect Your Devices

- Lock screens
- Encrypt devices
- Use antivirus/endpoint protection
- Avoid public Wi-Fi without a VPN
- Remove unused apps/software

Monitor Your Accounts

- Check bank statements
- Review credit reports
- Set up fraud alerts
- Watch for unexpected password reset emails