Protecting Yourself When True Privacy Is Impossible

The Fake Call That Seemed Too Real

It started with a phone call that seemed completely ordinary. “Hello, Mrs. Patel? This is Michael from your bank’s fraud department. We’ve noticed unusual activity on your account. Did you recently make a $1,200 purchase at an electronics store?” Mrs. Patel’s heart skipped. She hadn’t bought anything like that.

To make things more convincing, “Michael” confirmed her home address and her birth date — information she assumed only her bank would know. He explained that to reverse the charge she would need to verify her identity by providing her credit card details and bank login and password. Feeling anxious, she did as he asked. The caller thanked her and assured her the issue would be fixed, but a few hours later, Mrs. Patel could no longer access her bank account. Then she started getting notifications of thousands of dollars being transferred overseas from her account.
What Mrs. Patel did not realize was that the scammer had obtained her personal information from a previous data breach and used it to sound credible. Everything about the call was fake. She had just been scammed.

Our Data is Everywhere

In today’s connected world, privacy has become one of the hardest things to protect. Every time we shop online, stream a movie, use a credit card, drive on the highway, or use a mobile app, our information is being collected, analyzed, and shared. In addition, much of our personal data may be a matter of public record, stored in government voter registration databases, tax records or data on home purchases. Even something as simple as walking in a parking lot can involve being recorded by security cameras in most modern cars.

Regardless of who is collecting the information or why, the result is the same: A massive amount of personal information is stored in databases around the world, which is data you have no control over. And once that data exists, it can be stolen, sold, shared or misused. Achieving true privacy is nearly impossible.

Just Because They Know You Doesn’t Mean They’re Legitimate

Attackers often use all of this accessible information about you to make their scams more believable. For example:

1. A scammer might call you pretending to be from your bank and confirm your home address before asking for your login and account number.
2. An email may include your full name, phone number, and birth date to appear legitimate.
3. A text message may look like it's from a car warranty service, complete with details about the make, model, and year of one of your cars.

The truth is, having personal information about you doesn't make someone trustworthy, it only makes them more convincing. Always treat unexpected messages, calls, and emails with skepticism, no matter how much the sender seems to "know" about you or how urgent the message feels. Always feel comfortable hanging up and calling the institution on a trusted phone number that you know to be legitimate.

Watch Over Your Money – This is Where Fraud Begins

Since you can't protect all your information, the next best line of defense is **early detection**. Monitoring your financial accounts gives you a critical advantage: You can catch suspicious activity before it causes real damage. The faster you notice a fraudulent charge, the easier it is to reverse it and prevent further losses. Here are simple steps anyone can take:

- **Set up alerts:** Most banks, credit cards, and investment services allow you to receive instant text messages for every transaction, withdrawal, or login attempt.
- **Review your accounts regularly:** Even with alerts, take a few minutes each week to check balances and recent activity for anything unusual. Or perhaps configure your accounts to email you daily or weekly reports.
- **Freeze your credit:** Depending on your country, you may be able to freeze your credit so no one can take out a loan or credit card in your name. In addition, you can access free or low-cost reports from credit bureaus. Look for unfamiliar accounts or inquiries.

In today's world, perfect privacy is no longer achievable. Always remember that just because someone knows information about you does not make them legitimate. You don't need to be a cybersecurity expert to stay safe: just stay alert, ask questions, and keep watch over your accounts.

Guest Editor

Dr. Litany Lineberry, Secretary of the WiCyS Education and Training Affiliate, holds a Ph.D. in Engineering with a Cybersecurity focus. She teaches Information Systems Technology courses at Hinds Community College, Utica Campus, and supports WiCyS' mission to recruit, retain, and promote women in cybersecurity across all sectors. https://www.linkedin.com/in/litany-lineberry

Resources

How Cybercriminals Exploit Your Emotions: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
How Cybercriminals Steal Your Passwords: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
Locking Down Your Financial Accounts: https://www.sans.org/newsletters/ouch/dont-let-cybercriminals-swipe-your-savings-lock-down-your-financial-accounts/

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch