West Virginia Executive Branch
Privacy Tip

Identity Theft – Guard your numbers!



As you know, the Privacy Office occasionally issues tips to assist you in your "away from work" life. This tip is for that purpose.

You know that identity thieves are after your email addresses and passwords, social security numbers and bank account numbers, but that's not all they want. We are all attached to various sets of numbers that, when gathered together, allow high-tech identity thieves to get their hooks into you. They don't even need all of your information to cause problems. They just need enough to convince others that they are you. Here are several numbers that they are gunning for:

1. Phone Numbers

Putting your phone number on a public-facing site or even in a phone book could be risky. Identity thieves are looking for new ways to scam you, and calling you pretending to be a legitimate company is one of them.

According to the Federal Trade Commission's website (FTC Guide - Caller ID and Spoofing):

> Using a practice known as "caller ID spoofing," callers can deliberately falsify the telephone number and/or name relayed as the Caller ID information to disguise the identity of the calling party. For example, identity thieves who want to collect sensitive information such as your bank account or other financial account numbers, your social security number, your date of birth or your mother's maiden name, sometimes use caller ID spoofing to make it appear as though they are calling from your bank, credit card company, or even a government agency.

Remember-NEVER give any personal information to a caller saying they are from your bank, credit card company, etc. You should only provide this information if you have called them. Always use the contact information provided by the institution, don't rely on your caller ID box.

2. Dates and ZIPs

Birth, college attendance, employment, when you resided at a particular address, ZIP codes associated with open accounts—these are all numbers that can help a scam artist identity you, bit by bit. Many people put this information on public websites, like personal blogs and social media sites. In the post-privacy era, you must grasp the concept that less is more (remember "Minimum Necessary"? It applies to your own info!). Try populating your public-facing social media sites with inaccurate information – though you should check each site's rules, some sites frown upon the practice.

3. PIN Codes

Card-skimmers use a device to capture your debit card information while a camera records you as you type in your PIN code, making it very easy for a thief to replicate. Cover your hands and be paranoid, because it's possible someone actually is watching you.

4. Driver's License and Passport Numbers

These are critical elements of your personally identifiable information that represent major pieces of your identity puzzle and, once you have the number, these documents can be counterfeited. Millions of personal documents undergo major makeovers every day and suddenly feature new names, addresses and photographs of identity thieves.

5. Health Insurance Account Numbers

Health insurance fraud is on the rise, and one of the biggest growth areas is identity-related health care crimes. This can jeopardize your life – not just your credit or finances, as the identity thief's medical information can be commingled with yours, precipitating blood type changes, and eliminating certain allergies to medications or presenting new ones. The results can be catastrophic when a course of treatment is prescribed based upon incorrect information in the file.

It's time to become a data security realist. You should pay attention to newly reported data breaches and scams, as each may help you identify steps you can take to reduce damage and ways that your lack of personal data security might be putting you at risk. So don't ignore articles about new threats to data security – your data could be involved!

While there is no way to avoid cybercrime and identity theft, there is plenty you can do to make sure the damage is minimized and contained, and that no matter what happens, your daily life can go on without too much disruption.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.