SERVICE BRIEF

Understanding Your Virtual Identity

Protect yourself from online identity thieves.

Personally Identifiable Information

Social Security numbers, dates of birth, home addresses, and more.

We often talk about threats to business infrastructures, but the point stands that these same threats make advances on individuals as well. If enough personally identifiable information

is stolen, a hacker could completely lift the identity of a user to take out loans, hijack credit card numbers, and even infiltrate social media accounts to further spread their influence. The result could be a ruined credit score and a damaged reputation--a major problem for anyone, not just the business owner.

One thing to keep in mind is that a general best practice is to keep sensitive information as far away from the Internet as possible, and to only input such information into secured, verified sources. However, it's not always this simple. We'll discuss some of the most common ways that individuals can protect themselves against threats like identity theft.

This should go without saying, but Social Security numbers, dates of birth, addresses, and other sensitive information that directly identifies the user, should be used with discretion while on the Internet. Sometimes users might receive phishing emails from what appear to be banks or government agencies that request a "verification" of sensitive information. You should know that requests like these will never be sent via email or phone call, and will almost certainly be found in your home address mailbox.

Financial Credentials

Credit card numbers, PINs, CSCs, etc.

Financial information is in high demand for hackers. If they don't want to use your personal finances for their own purposes, they can sell your credit card credentials on the black market to make money that way. Either way, hackers will resolutely pursue your credentials. It's your responsibility to keep them away. Never store your financial credentials locally on your PC, and make sure that any site you're plugging them into is secured with encryption and a security certificate. You can check by looking for a green padlock icon, or https, in the browser's address bar.

Other Sensitive Data

Passwords, usernames, and more.

Login credentials are common targets for hackers, and they'll use every trick in the book to get them. Passwords and usernames are required for logging into accounts. In particular, hackers could access your email, social media account, online shopping accounts, and more, with the intention of stealing your identity or sensitive data. Using complex passwords and usernames is a great first step toward protecting yourself online, and using a consumer-grade password manager can help you use complex passwords without the need to remember them.

Sensitive Data

- Personal details, like date of birth, Social Security numbers, and addresses.
- Credit card data, like numbers, PINs, CSCs, as well as other financial account details.
- Login credentials, such as passwords, usernames, and security question responses.
- Health/Medical information.
- Easily-Transferable Digital File Formats

Threats

- Loan fraud
- Credit card fraud
- Property theft
- Identity theft
- Data Theft
- Email Access
- Damaged reputation

Get proactive and call us TODAY!

(808) 529-4605| indevtech.com | info@indevtech.com

Indevtech Incorporated
Pacific Guardian Center, Mauka Tower
737 Bishop Street, Suite 2070
Honolulu, Hawaii 96813-3205