Stay Vigilant: Nine Ways to Protect Your Personal Data

Unlike most risks, data breaches have the potential to negatively impact every consumer, every employee… everyone, every day.

Cybercrime continues to not only increase in incidents and victims but also in sophistication from the criminals and the tactics they deploy. Everyone must be hyper-aware of best practice daily habits we can deploy such as:

1. **Leverage Multi-Factor Authentication (MFA)**
   To reduce the chances of account intrusion, enable MFA when possible so you have to verify it's you on multiple, approved devices. Employees and employers should never share their multifactor authentication codes with anyone. isolved will never call and ask for it.

2. **Look for Signs of Malicious Intent**
   Whether it's misspellings, too-good-to-be-true offers, or anything similar, we must all consider everything we receive as having the potential to steal data—such as an email from an unknown sender that has your name incorrect or a text message from someone you weren't expecting a message from that is requiring some sort of action.

3. **Look for Signs of Trust**
   Many organizations exist that help keep people data safe by displaying trust signals such as "https" in a website's URL versus "http" or a lock in the URL field. While these are not foolproof security protocols, they are often signs of trust.

4. **Don't Be Overly Helpful**
   For the most part, people want to help people. Bad actors prey on this belief by texting employees, for example, that the "CEO" is in need of an important document—urgently. Another common example of a scam that can lead to your data being stolen is text messages from unknown senders where people respond back with more information than they should ("this isn't Michael but it is Michelle…). Be cautious with all communications you were not expecting and verify with the person directly before being helpful.

5. **Do Not Store Passwords or Reuse Them Often**
   Whether it's a sticky note on your computer or a digital file on your computer, it's critical that you don't save passwords that can be intercepted and used by anyone other than you. What's more, it's important to use unique passwords rather than reuse them.

6. **Use Caution Before Clicking & Scanning**
   With businesses trying to get our attention via email, social and a variety of other channels, it's easy to fall victim to phishing schemes—when a bad actor appears to be a reputable business. Use common sense such as reviewing the materials before clicking on a link, scanning a QR code or even applying to a new job position.

7. **Monitor the Dark Web & Your Credit Report**
   Plenty of services exist that will alert you if your login information, name, email address, home address or other personally identifiable information (PII) is released on the dark web. Similarly, credit monitoring agencies can alert you of any new accounts or activity that you should be aware of.

8. **Educate Yourself**
   While security training may get a bad reputation from videos from the '90s and early 2000s, it's come a long way and is often updated to include the latest tactics bad actors are using to try and gain access to your data. If your employer offers security training—take it, even if it's not mandatory.

9. **Support the Security Cause**
   Don't be part of the problem but part of the solution instead. At work, for example, follow policies and procedures to protect yourself and your coworkers—whether that's not leaving your device unattended, taking security training, wearing your badge or ensuring no unexpected visitors enter the office.

Discover how isolved protects your data by visiting isolvedhcm.com/trust-center or scanning the QR code.

Disclaimer. The information provided herein is for general informational purposes only and is not intended to be legal or other professional advice, including data privacy and security advice. All information discussed is of a general nature and does not address the circumstances of any particular individual or entity. We make no representation that the content will guarantee prevention of cyber incidents and disclaim all liability for actions you take or fail to take based on any content we provide. There is no form of relationship formed by any use of this information. The accuracy, completeness or adequacy of the information is not guaranteed, and isolved assumes no responsibility or liability for any errors or omissions in the content. It is not a substitute for legal advice or any other professional advice, including data privacy and security and you should not rely on it as such. You should consult with an attorney, or other appropriate professional for advice regarding your specific situation.