Your Identity Theft Playbook

The United States suffers identity theft at more than twice the rate of the world average. According to a recent survey, identity theft has struck an astonishing 33 percent of US citizens. And, while thieves certainly prey on the elderly, the majority of victims are younger. Consequently, identity theft poses a risk not only for the victim, but for their places of business.

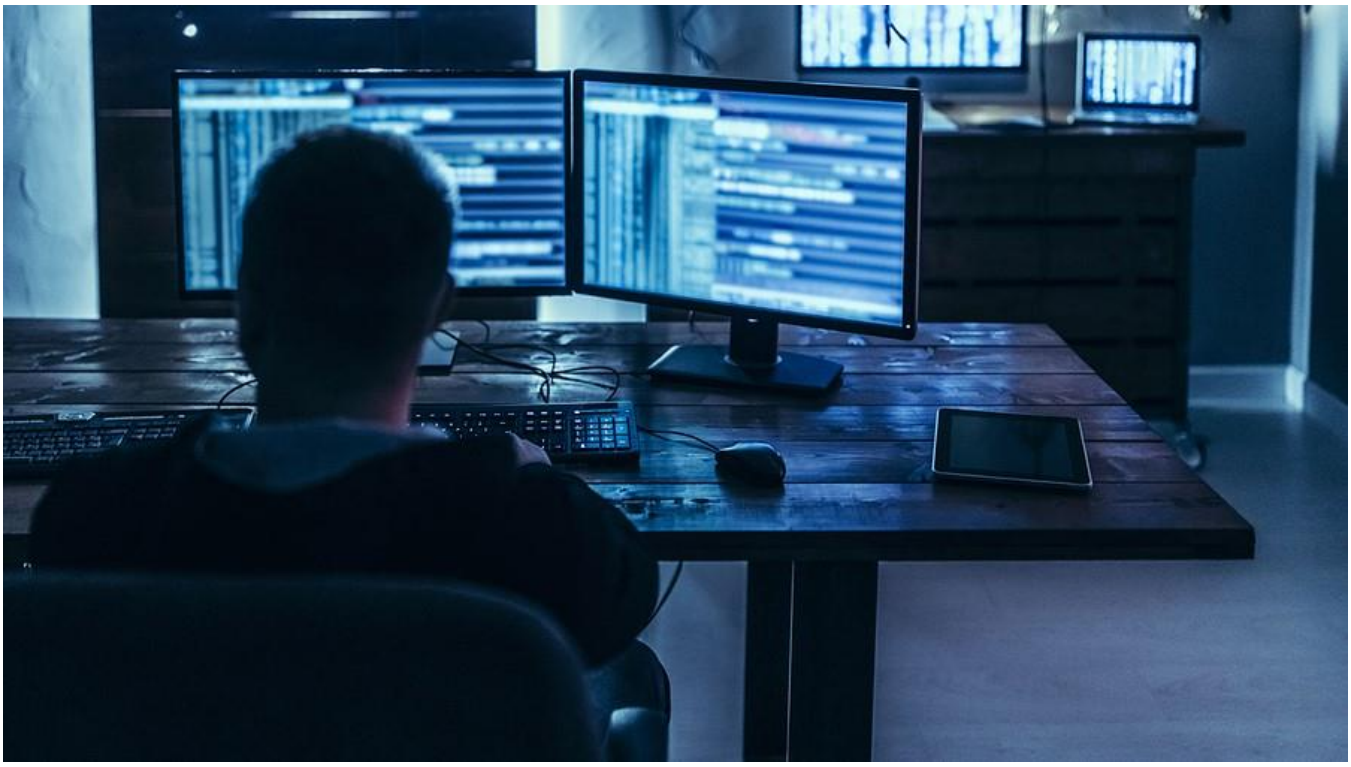
Consider the risk when high-level employees have their identities stolen. Not only can thieves wipe out their bank accounts, but they can use stolen credentials to gain access to privileged information. Individuals and businesses both need to be aware of the signs and dangers of identity theft and how to respond.

Signs of Identity Theft

Identity thieves can gain access to sensitive personal information in a variety of ways. A data breach at a place you do business can expose your data. Or bad actors may gain access to your phone or computer. Regardless of the access point, you may not know that your information has been compromised.

However, a few telltale signs can provide a warning to look deeper. For example, fraudulent credit card purchases often give the first clue. Likewise, unfamiliar bank account activity suggests unauthorized access.

Additional signs include unfamiliar bills, loss of cellphone service and denied medical claims. These indicate someone has used your name to open accounts. Likewise, arrest warrants or the inability to file taxes because the IRS already has a return filed in your name both indicate identity theft.



Mobile Danger Zone

Cell phones prove especially attractive targets for identity thieves, as they contain a treasure trove of valuable personal information. Despite carrying sensitive data and links to financial accounts, many users fail to protect their phones properly. Learn how to protect your phone from hackers and how to recognize when your phone has been hacked.

What to Do When Identity Theft Strikes

When you notice signs of theft, take steps to change your digital identity to protect both your business and you. Start with the steps outlined below.

Protect your business

1. Change your identity across access control systems – In the access control systems for Microsoft 365, your ERP system, and so forth, change the primary authentication method. That is, instead of listing your compromised email address, create and use a new email address as the authentication method.

   Then, move the original email address to a distribution group. Within minutes of doing this, hackers will be unable to use an automated hacking tool against you. This will involve no change to how outside users connect with you. You can still receive email at your original email address.

2. Implement a honey pot – A honey pot is an account that looks legitimate but will notify security personnel of any activity. Thus, if a bad actor tries to authenticate through the honey pot using your compromised email, security personnel know to block their access.

3. Mobile Device Management (MDM) – An MDM system allows IT to specify which devices can access the network and what applications they can access. Additionally, if someone steals an employee cell phone, IT can remotely wipe the phone to protect privileged access.

4. Dark Web scanning – Thieves typically sell stolen credentials on the Dark Web, a network of often shady digital communities. A Dark Web monitoring service will proactively monitor for data stolen from your organization.

Protect your personal identity

1. Create alias email addresses for authentication – Avoid using your primary email as the authentication for social media or other accounts, such as your bank account. Instead, create separate alias email addresses as authentication IDs for each account. That way, if one site's credentials become compromised, the remaining accounts remain safe.

2. Change your Apple ID password immediately – As soon as you discover a lost or stolen phone or a compromised email, change your Apple ID password. Also change the identity you use to authenticate your Apple ID.

3. Implement additional cell phone security – Many of the same security tools that you use to protect business computers work for your phone, as well. Start by adding antivirus and anti-malware. You can also implement a DNS security service and a phone VPN connection to the office.

4. Change your primary phone number – For additional protection, you can create a virtual phone number using a service such as Digits or Google Voice. The virtual number can forward directly to your phone or email. This allows you to keep your actual phone number private, only giving it to trusted individuals.

Implement Your Identity Theft Playbook with Expert Help

The cybersecurity experts at eMazzanti have the tools you need to keep your identity and your business safe from hackers. They will help you implement multi-layer security, including mobile security, network security and Dark Web scanning. Call us today for a free cybersecurity assessment.