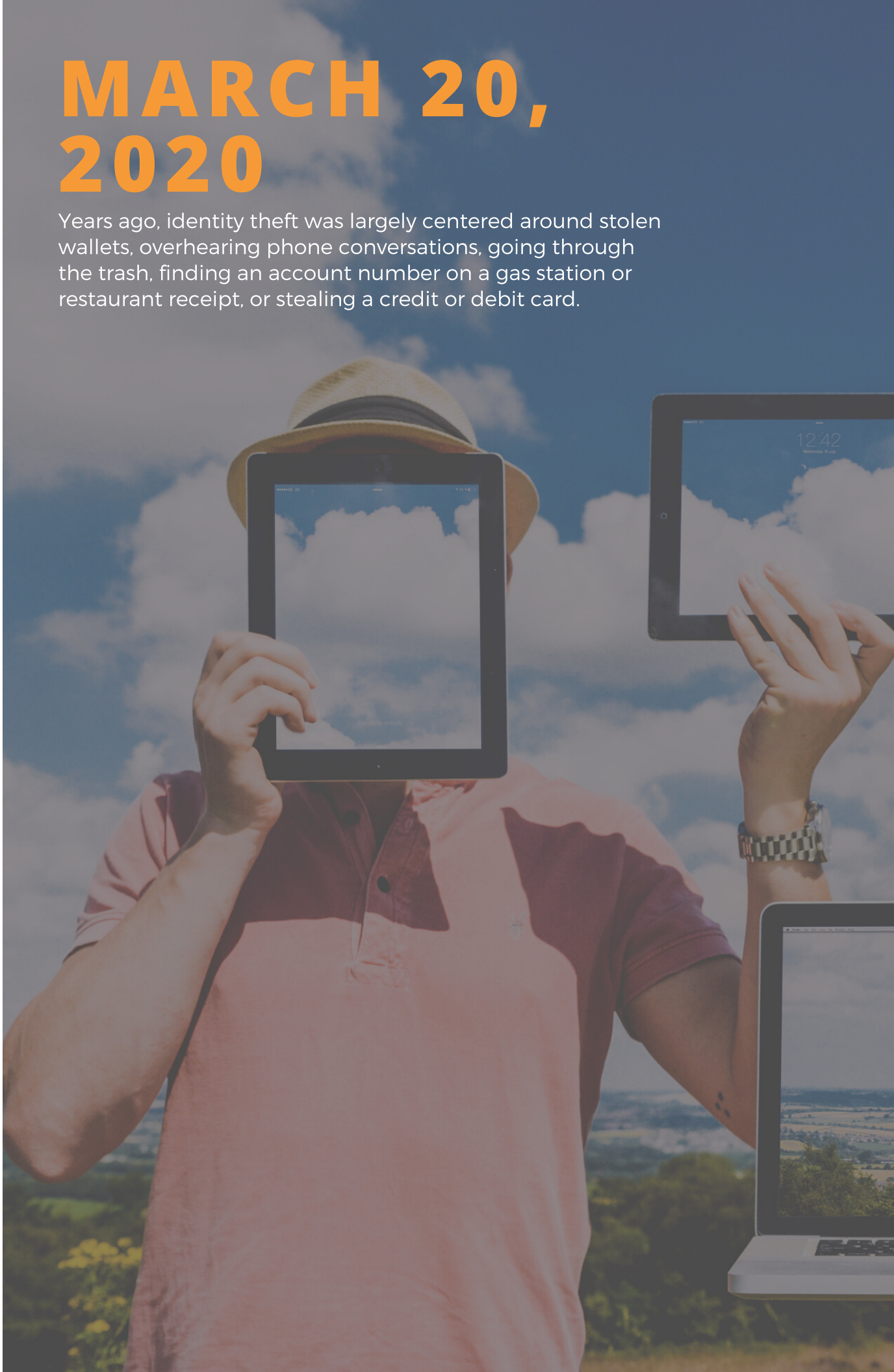
MARCH 20, 2020

Years ago, identity theft was largely centered around stolen wallets, overhearing phone conversations, going through the trash, finding an account number on a gas station or restaurant receipt, or stealing a credit or debit card.



Security First IT

IRS FRAUD - HOW TO SPOT IT AND NOT FALL FOR IT!

Don't be left hanging high and dry - and with an empty bank account.

Like other crimes, identity theft is largely a crime of opportunity.

Years ago, identity theft was largely centered around stolen wallets, overhearing phone conversations, going through the trash, finding an account number on a gas station or restaurant receipt, or stealing a credit or debit card.

However, with the amount of sensitive information that is stored online today, it has grown easier to become a victim of identity theft through no direct choice of your own. Business and government databases are an attractive bait for cybercriminals, as this information is useful in many applications, be them for malicious, research, or business reasons.

What is phishing? Phishing is a scam carried out through unsolicited email or spoofed websites, used to collect a victim's personal information such as social security numbers and bank account information.

SIt is one of the most common forms of cybercrime. IRS Contact Methods The IRS will only contact an individual via postal mail. They will not contact an individual through email, text messages, social media channels, or over the phone. This is for any reason including access to banking information, PINs, return information, etc.

Important Reading:

- Publication 4524, Security Awareness for Taxpayers (PDF)
- Publication 5027, Identity Theft Information for Taxpayers (PDF)

Want to join in the conversation? Talk with us on social media!
Facebook: https://www.facebook.com/secfirstit/
LinkedIn: https://www.linkedin.com/company/securityfirstit

Hashtags: #irs #fraud #tax fraud #fraud watch #irs fraud #irs fraud call #irs scam #bank fraud

Help! I Think A Fake IRS Agent Just Emailed Me!

For Individuals:

If you receive an IRS phishing email, follow these steps.

1. Do not reply. Replying gives the criminal additional chances to access personal information and verifies that you have received their email.
2. Do not open any links or attachments, either on a PC or mobile device – the attachment or link may contain malicious code.
3. Do not enter any personal information. If you are concerned that some of your personal information has been compromised, visit the IRS' identity protection page.
4. Forward – with all original information - the email to phishing@irs.gov.
5. Delete the original email and anything that was downloaded from it. I've Received General Phishing/Spam!

For Businesses:

If you receive an IRS phishing email, follow these steps.

1. Do not reply. Replying gives the criminal additional chances to access personal information and verifies that you have received their email.
2. Do not open any links or attachments, either on a PC or mobile device – the attachment or link may contain malicious code.
3. Do not enter any personal information. If you are concerned that some of your personal information has been compromised, visit the IRS' identity protection page.
4. Forward – with all original information - the email to reportphishing@antiphishing.org.
5. Delete the original email and anything that was downloaded from it.

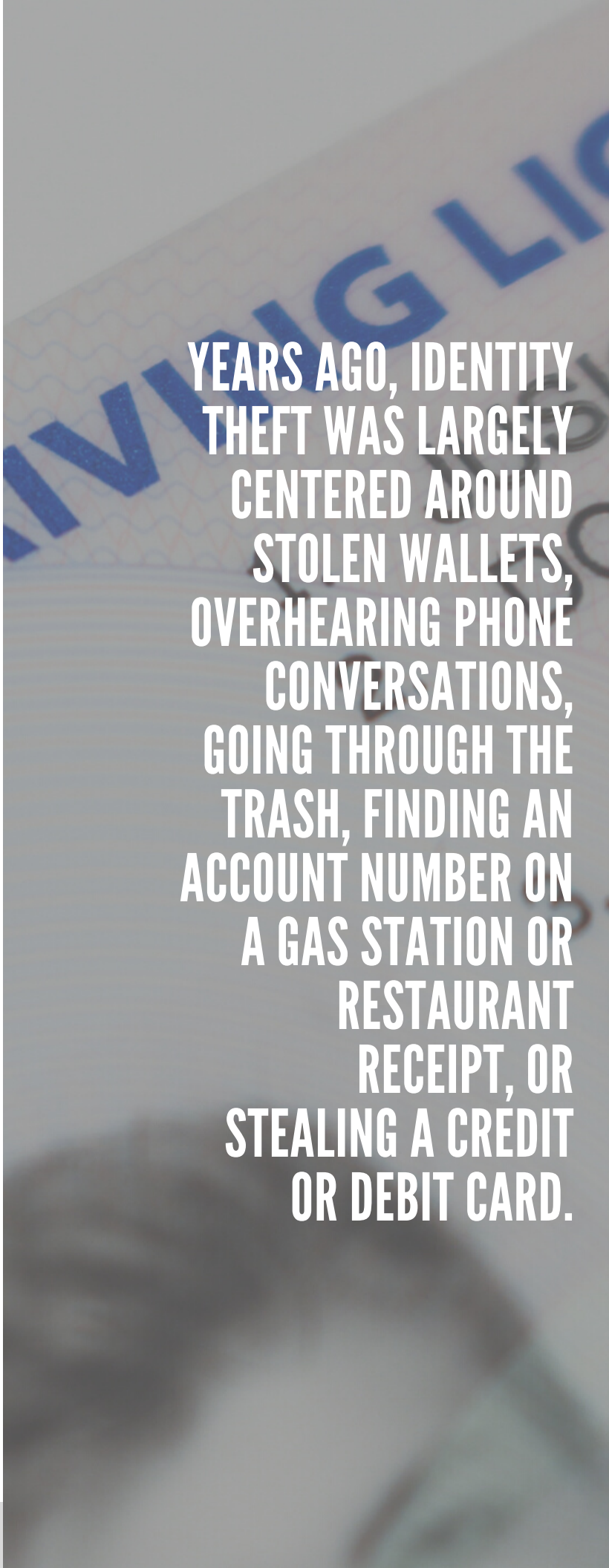
If evidence indicates that your personal information has been used to gain wages through an employer that you do not work for, reference the Guide to Employment-Related Identity Theft.

Help! I Think A Fake IRS Agent Just Texted/Messaged/Called Me!

IRS spoofing calls fall in line with other robocalls such as fake tech support, sweepstakes, bill collectors, contests, legal calls, and others. These calls are popular and widely used by scammers, as they use scare tactics to convince the victim to give their information to the scammer on the line.

Text: If you receive an IRS phishing test message/SMS, follow these steps.

1. Do not reply. Replying gives the criminal additional chances to access personal information and verifies that you have received their message.
2. Do not open any links or attachments – the attachment or link may contain malicious code.
3. Do not enter any personal information. If you are concerned that some of your personal information has been compromised, visit the IRS' identity protection page.
4. Forward the text, with nothing added, to 202-552-1226. (This is the IRS' text reporting line.)
5. In a separate text, forward the originating number to 202-552-1226. (This is the IRS' text reporting line.)
6. Delete the original text and block the number it was sent from.



Phone Call: If you receive an IRS phishing phone call, follow these steps.

If you are suspicious that an individual you have spoken with over the phone is not affiliated with the IRS:

- View your tax account information online via the IRS portal to review the amount owed to verify if the information expressed during the phone call matches.
- Place a return call using appropriate online resources via the IRS portal to verify.

After listening, do not give any information and terminate the call. Collect any necessary/pertinent information.

- The telephone number of the caller.
- The telephone number you were given to call back.
- A description of the conversation.

If possible include:

- The employee's name.
- The employee's badge number.
- The exact date and time that you received the call(s.)
- The geographic location and time zone where you received the call.

Also consider filing a complaint with the:

- Federal Trade Commission (FTC)FCC
- Consumer Complaint Center
- Treasury Inspector General for Tax Administration
- Your state's attorney general

Take-Away: There are a few call-screening apps available. Check out these great resources: Consumer Reports, Consumer's Union, CTIA, and Indiana AG.

How Do I Verify Contact with the IRS?
Use the IRS.gov website to search the identification number printed on the letter, notice or form number.
All printed material from the IRS will contain instructions on how to properly contact the IRS.

If there is still doubt, use the forms and instructions function on the IRS website to match the forms you received with the forms available on the website.