

CREATIVE DESIGN

imagine the possibilities.

Design

East Cambridge Savings Bank Tri-Fold Brochure Contest

WHAT IS IDENTITY THEFT?

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else.



VISIT OUR WEBSITE
WWW.ECSB.COM

FACEBOOK
EASTCAMBRIDGESAVINGSBANK

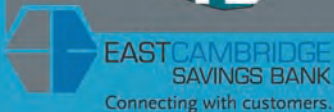
CALL US
1-(866)354-ECSB
1-(866)354-3272

EMAIL US
CUSTOMERSERVICE@ECSB.COM

BUSINESS HOURS
MONDAY - FRIDAY: 9AM - 6PM
SATURDAY: 8:30 AM - 1PM
SUNDAY: CLOSED

PROTECTING YOURSELF AGAINST IDENTITY THEFT

BE ALERT TO THE SIGNS OF IDENTITY THEFT. A SCAMMER MAY TRY TO OBTAIN YOUR PERSONAL INFORMATION BY ASKING YOU TO PROVIDE IT TO THEM.



1st Place Winner
Anne Pierre



PROTECT YOURSELF AGAINST IDENTITY THEFT

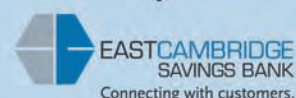
WHO AM I WITHOUT MY IDENTITY?

Contact Us

- Monday-Friday: 9 AM - 6 PM
Saturday: 8:30 AM - 6 PM
- Facebook.com/
EASTCAMBRIDGESAVINGSBANK
- Call Us:
1(866) 354-3272
- Email Us:
CUSTOMERSERVICE@ECSB.COM



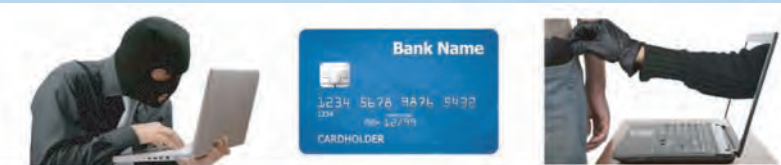
FOR MORE HELP OF INFORMATION
GO TO
WWW.IDC.GOV
OR CALL THE FDIC TOLL-FREE:
1 (877) 275-3542



CYBER SECURITY CHECKLIST

10 SIMPLE THINGS BANK CUSTOMERS CAN DO TO HELP PROTECT THEIR COMPUTERS AND MONEY FROM CRIMINALS.

1. KEEP ALL SECURITY PROGRAMS REGULARLY UPDATED.
2. CONNECT TO SECURE WI-FI SOURCES WHEN ONLINE BANKING.
3. USE INTERNET SAFETY FEATURES.
4. IGNORE UNKNOWN EMAILS OR LINKS.
5. DON'T GIVE OUT YOUR PERSONAL INFORMATION.
6. USE MORE THAN ONE SECURE PASSWORD.
7. BE CAUTIOUS OF THE INFORMATION YOU PUT ON SOCIAL MEDIA.
8. BE MINDFUL OF THE INFORMATION ON YOUR MOBILE DEVICE.
9. TEACH OTHERS ABOUT CYBER SECURITY.
10. SMALL BUSINESS OWNERS SHOULD TRAIN THEIR EMPLOYEES ON CYBER SECURITY.



- Keep all security programs regularly updated
- Connect to secure wi-fi sources when online banking
- Be cautious of information you put on social media
- Be mindful of the information on your mobile device
- Small business should train their employees on cyber security
- Use internet safety features
- Use more than one secure password
- Don't give out your personal information
- Teach others about cyber security
- Ignore unknown emails or links

- Install anti-virus software to protect against malicious software.
- Cybercriminals are good at creating fake emails that look legit.
- Wifi networks / computers as libraries or hotels can be risky if they don't have up-to-date security.
- A safe strategy is to ignore unsolicited request for information.
- Create "strong" password that are hard to guess and change them regularly.
- Criminals look for information such as someone's date of birth and through social networks which can help them guess passwords.
- Don't leave your mobile device unattended and use a device password if it's stolen or lost.
- Talk to your child about being safe online, including the risk of sharing personal information.
- Consider requiring more information beyond a password to gain access to your business's network.

3rd Place Winner
Jaryd Wallace

HAVE POLICIES FOR EMPLOYEES ON IDENTITY THEFT PROTECTION

Things like more information and safety measures should be required to gain access to your business's network, anything more than just a password. An example is confirmation calls or codes with your financial institution before certain electronic transfers are authorized.

HAVE COMPUTER SECURITY

Install anti-virus software and have a firewall to protect from unauthorized access to your computer. Without it, there are potential threats to your important information being stolen, like passwords and account numbers.



Facebook.com/EastCambridgeSavingsBank



1+866-354-ECSB (3272)



www.ECSB.com

Open 8:30-5 Monday-Wednesday
Open 8:30-6 Thursday-Friday
Open 9-1 Saturday
Closed Sunday



PROTECTING YOURSELF FROM IDENTITY THEFT



2nd Place Winner
Billy Nicolas

If someone were to take your identity, they could spend your money, message people you know and basically be you! Also, they now have access to everything you've ever done including things you have bought, things you have sent, and things you have done.

BE SMART WHEN CONNECTING THE INTERNET WITH BANKING

Public Wi-Fi networks and computers can be risky because they may not have up-to-date security software and firewalls.

SAFEGUARD YOURSELF

Look for a padlock symbol when banking or online shopping, as that means it's secure. Also, look for "https://" at

the beginning of a Web address, as that means it is authentic and encrypts data during transmission.

BE DISCREET WHEN USING SOCIAL MEDIA

Criminals will often look on websites like Facebook and Twitter for things like parents names and pet names, as this could help to figure out passwords.

IGNORE EMAILS ASKING FOR YOU TO OPEN ATTACHMENTS

Cybercriminals are good for creating fake emails that look legit, but could potentially install malware. Be sure to ignore those emails and to inform somebody that you received that kind of email and delete the email afterwards.

USE SECURE PASSWORDS

Create "strong" passwords that are hard to guess, change them regularly, and try not to use the same passwords or PINs for several accounts.

DON'T GIVE OUT PERSONAL INFORMATION

Ignore any messages, regardless of how legitimate they may seem, that may ask for personal information, especially things like Social Security and bank information.

INCLUDE CHILDREN IN CYBERSECURITY

Talk with your child about the dangers of sharing personal information with strangers and make sure their devices have up-to-date security.

