SeacoastBank®

PROTECT YOURSELF FROM SCAMS & FRAUD

TABLE OF CONTENTS

THREE MOST COMMON TYPES OF FRAUD

IDENTITY THEFT

IMPOSTER SCAMS

ONLINE SHOPPING & NEGATIVE REVIEWS

Dunn, A. (2022, September 7). *Financial Health Pulse® 2022 U.S. trends report*. Financial Health Network. Retrieved November 10, 2022, from https://finhealthnetwork.org/research/financial-health-pulse-2022-u-s-trends-report/

PHISHING: AN INCREASING THREAT

30% Approximately **1 in every 99 emails** is a phishing attack, and about 30% of those make it past default security.

47% **LinkedIn** phishing messages make up 47% of social media phishing attempts.

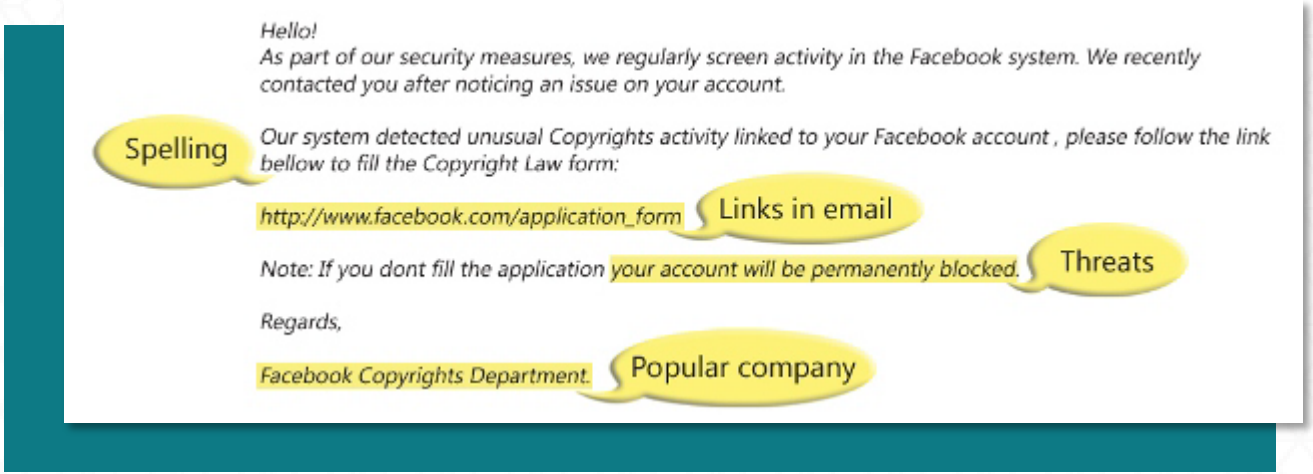
Most phishing emails commonly contain malicious files or links:

- **Spoofed links** trick you into entering your **login credentials** into a look-alike website. Those credentials are then harvested.
- **Malicious files** automatically download or install files that provide the attacker **prolonged access** to the system.

Sources: https://smallbiztrends.com/2019/07/phishing-statistics.html, https://www.cobalt.io/blog/top-cybersecurity-statistics-for-2022, https://www.infosecurity-magazine.com/news/covid19-massive-q1-phishing/, Phishing, Smishing and Vishing: What's the Difference? - Experian

PHISHING EMAILS: THINGS TO LOOK FOR

Here is an example of what a phishing scam in an email message might look like:



Beware of links. When you hover over it (don't click) does it match the senders name?

https://www.seacoastbank.com/resource-center/blog/how-to-recognize-a-phishing-scam

SMISHING: FRAUDULENT TEXTS

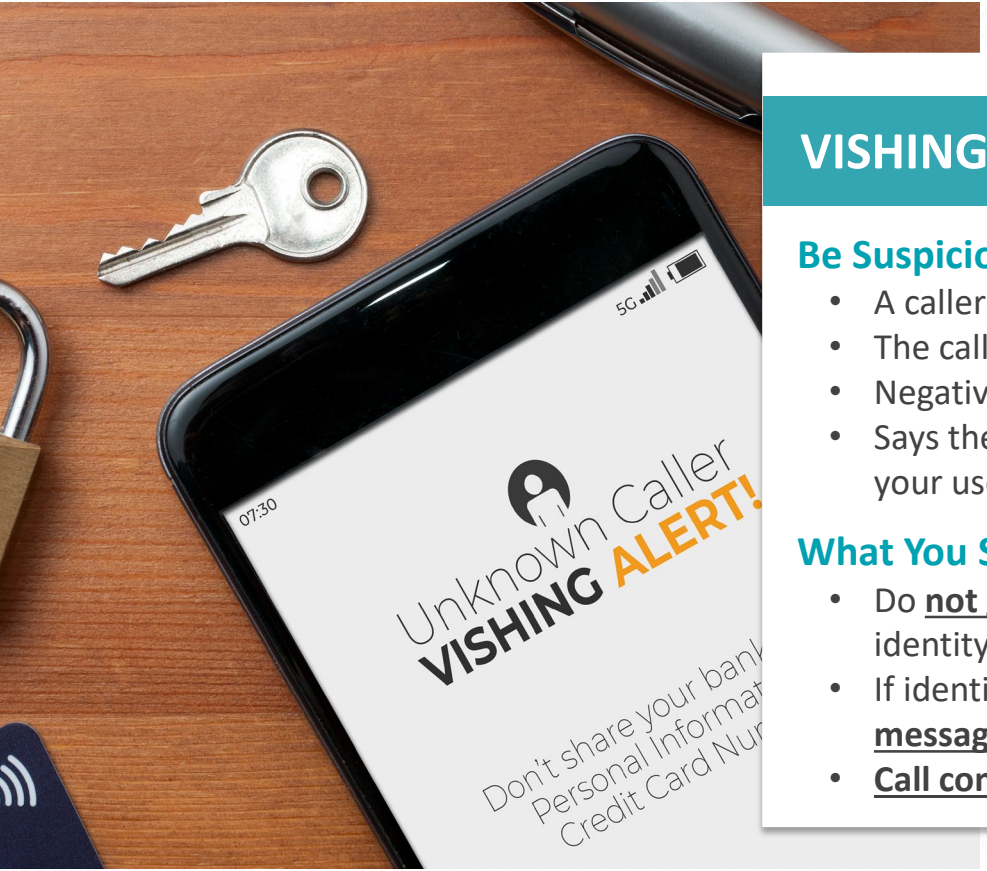
Be Suspicious of text messages when:

- Unusual or unexpected
- Requests a reply
- Requests unusual information or action
- Unfamiliar number
- Urgent
- Sender is unavailable to talk to you directly
- Unusual for you to receive a text from the sender

What You Should Do:

- **Not reply**
- **Call the supposed sender** at a known number
- **Contact someone** else who can confirm sender's location if sender is unavailable

Phishing, Smishing and Vishing: What's the Difference? - Experian



VISHING: VOICE PHISHING

Be Suspicious When:

- A caller requests information about you or your family
- The caller expresses a sense of urgency
- Negative consequences could result if action is not taken
- Says they are an employee of a company and requests your username or password or other sensitive information

What You Should Do:

- Do **not give any information** to caller without proper identity verification
- If identity cannot be validated, tell caller you will **take a message or call them back**
- **Call company** at a known phone number

Phishing, Smishing and Vishing: What's the Difference? - Experian

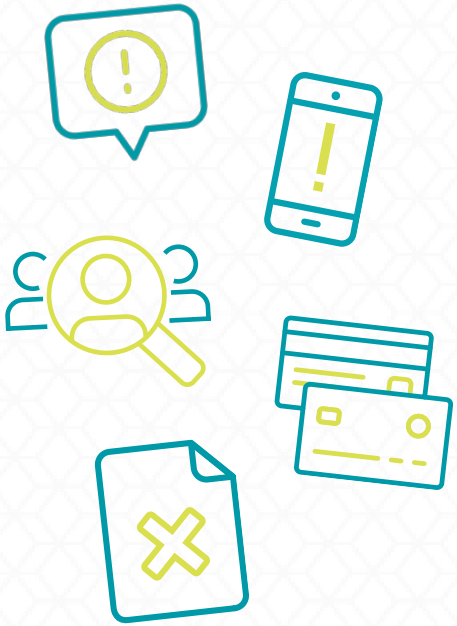
HOW IS YOUR PERSONAL INFO USED?

Personally Identifiable Information (PII) is any piece of information meant to identify a specific individual.

Scammers can use this info to:

- Change your address and order a new credit card
- Open new accounts
- Establish cell phone service in your name
- Drain your checking and savings accounts
- Take out a loan or mortgage in your name
- Wire fraud
- File a fraudulent tax refund
- Give your name when arrested
- Apply for a job
- Receive medical treatment/medical fraud

SIGNS YOUR IDENTITY MAY HAVE BEEN STOLEN



- Fraudulent charges on your credit card statement
- Credit card or bank paper statements not arriving (if applicable)
- Bills arrive for goods or services you did not request/purchase
- Suspicious inquiries on your credit report
- Phone calls from creditors
- Suddenly denied credit

PROTECT YOURSELF FROM FRAUD

- Set up **account alerts** to notify you of potentially fraudulent activity
- **Be cautious** when revealing your User IDs and passwords online, including on financial websites that provide tools for financial management, investing and tax preparation
- **Regularly check** your account transactions and balances
- **Shield your PIN number** when using it and do not leave your receipt at the ATM, gas pump or other retail location
- **Use strong passwords** and change them regularly

IF YOU SUSPECT YOUR IDENTITY IS BEING MISUSED

What to do:
File a police report, obtain a case number and request a copy of the report
File a complaint with the Federal Trade Commission: **877.438.4338**
Close all accounts that were affected ASAP
Call Social Security Administration: **800.772.1213**
Call United States Postal Inspector: **877.876.2455**
Keep a detailed log and keep copies of all correspondence
Place fraud alerts on all your accounts and with the credit reporting agencies

HOW TO PLACE A FRAUD ALERT

- Contact **one** of the credit bureaus
- Make sure they have your current contact information
- Placing a fraud alert allows you to receive one free credit report from each credit bureau
- The fraud alert will stay on your record for one year

Equifax
Equifax.com/personal/credit-report-services
800.685.1111

Experian
Experian.com/help
888.EXPERIAN (888.397.3742)

Transunion
TransUnion.com/credit-help
888.909.8872

Always question everything, from phone calls to mail solicitations to emails to social media links. If you're not 100% confident that the person and reason are legitimate, do not share."

CONNECT WITH US

ONLINE ANYTIME

Visit us online at
SeacoastBank.com

CUSTOMER SUPPORT

Call us at **800.706.9991**
Mon - Fri | 7am - 10pm
Saturday | 8:30am - 5pm
Sunday | CLOSED

SCHEDULE AN APPOINTMENT

Scan the QR code to meet with a representative near you to discuss your financial needs.

SeacoastBank®

THANK YOU

for your time.