Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation
&
BROADWAY BANK

What is Smishing?

Combating text-based phishing attempts

Have you been "smished"? You might be familiar with the term "phishing" (see another one of our resources titled *Phlushing Phish*). That is when scammers try to get your personal information by sending fraudulent links to you by email. Smishing is a term referring to phishing attempts that happen on your phone via text messages. **According to Norton Security, smishing attacks have increased 300% in the last two years.**

Your phone is an important, convenient tool. People are increasingly reliant on all the functionality that a phone can pack into your fingertips. Scammers understand that phones are increasingly where more commerce happens. Therefore, they know that it is likely there are passwords in your phone they'd like to get a hold of, along with your credit card information and any other personal data that could be used to steal your identity. They want access to data about you that is stored in apps that you use for things like banking and shopping.

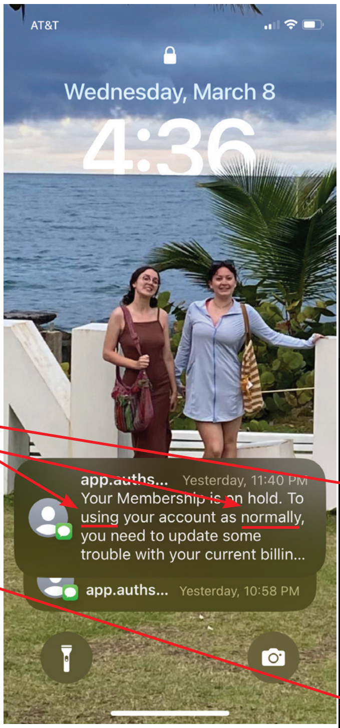
You'll find some of the characteristics of smishing resemble those of phishing attempts.

- Word often misspelled
- Grammar errors
- Refers to an account you haven't used lately
- Package/product you didn't order
- Urges you to act fast
- Originates from unknown phone number frequently repeated, often late at night – phone numbers might not be formatted in the typical way
- Weird looking links that don't match name

Smishing attempts tend to fall into certain categories:

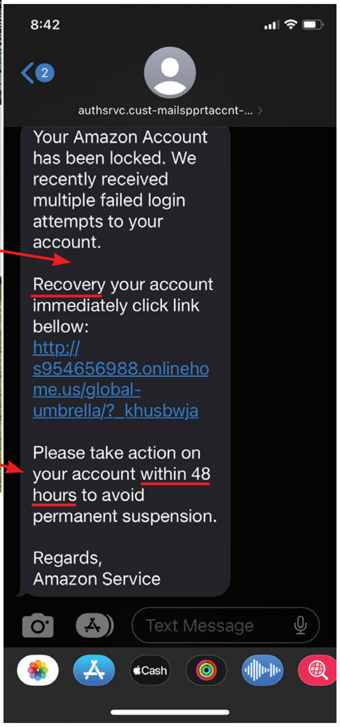
You've Won! If you've received a "Congratulations" message, you'll be familiar with this scam. This tactic advertises a fake contest giveaway you've won and try to get you to click on a malicious link to claim your prize. Once you continue to their site, malware could make its way onto your device and compromise your system and the information attached. Example: Be the first person to visit this link and win a free gaming system!

Confirmation smishing scams use fake confirmation requests to get you to compromise sensitive information. This could be for an online order, an upcoming appointment, or an invoice for business owners. The message may contain a link directing you to a site that asks you to input login credentials or other sensitive data to verify your appointment or purchase.



app.auths... Yesterday, 11:40 PM
Your Membership is on hold. To using your account as normally, you need to update some trouble with your current billin...

app.auths... Yesterday, 10:58 PM



Your Amazon Account has been locked. We recently received multiple failed login attempts to your account.

Recovery your account immediately click link bellow:
http://s954656988.onlinehome.us/global-umbrella/?_khusbwja

Please take action on your account within 48 hours to avoid permanent suspension.

Regards,
Amazon Service

What is Smishing?

continued from page 1

Customer support smishing scams send smishing texts posing as any company a person may trust – not just banks or credit card companies. They may pose as representatives from online businesses or retailers notifying you of an issue with your account. They'll provide directions to solve the issue, which typically includes you going to a fake site infected with spyware to record any information you type in.

Financial/banking services smishing scams leverage the fact that more and more people are managing their finances online. These smishing messages pose as legitimate and trustworthy banking institutions to get you to compromise sensitive data like Social Security numbers, addresses, phone numbers, passwords, and emails. Example: ATTENTION! Reactivate your credit card at this link NOW.

Tips

- Have a locking code or face ID activated on your phone
- Don't store sensitive information like passwords, credit card numbers and social security numbers on your phone.
- Don't click links!
- Don't use public wifi, especially if you are using a credit card for a transaction, or entering sensitive personal info. Hackers can intercept your data from these networks.
- Don't set up apps to automatically log you in, and be sure to log out of apps once you are done using them.
- Always keep track of your phone – don't leave it out where just anyone could access it. Consider loading the Find my iPhone app or Lookout for Android phones to help you find a phone if one goes missing.
- If your phone does disappear, call your phone provider and let them know it is lost or stolen. If you did happen to store credit card or other sensitive information on your phone, contact your bank or card servicer immediately.

Smishing Attacks Explained

Hackers can commit smishing in three simple steps.

1 **A hacker sends out a text infected with a malicious link.**

2 **You open the text, click on their link, and provide personal information.**

3 **The hacker uses your information to commit fraud or make a profit.**