Cyber-Savvy Seniors

Content brought to you by:

Senior Housing Crime Prevention Foundation

&

BROADWAY BANK

PHLUSHING PHISH

Recognizing and avoiding fraudulent attempts to obtain your sensitive information

No – don't flush the pet goldfish! What we are talking about here is Phishing. That is a cybercrime where targets are contacted by phone, online, email, or text message by someone posing as a legitimate institution, or someone you know to lure you into providing sensitive data like personally identifiable information, banking and credit card details, and passwords. The Phishers then use the personal data to access important accounts. This can result in identity theft as well as loss of money or property.

What Lures catch the most Phish?

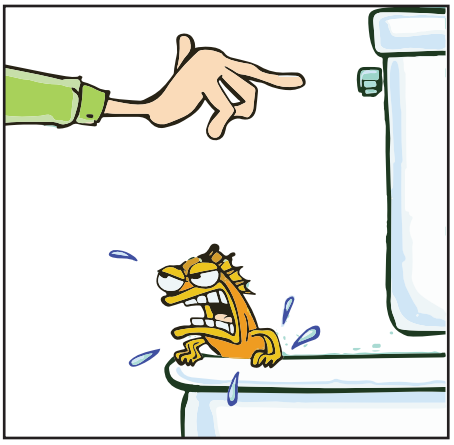
- Company or family names that sound familiar.
- Links to click to enter banking info or passwords. Either the info is stolen directly, or the links install malware that infect your computer and steal other information found there.
- Pressure tactics to hurry you into thinking if you don't act quickly there will be negative consequences.

Don't get hooked; do your research.

- You can always end a conversation and turn around and call the entity that reached out to you to determine if it is legitimate or not.
- You can ask the caller for a number to call back, but you need to look up the real customer service number for the bank or credit card or whatever entity the caller claimed to represent.
- Know that the IRS never makes outbound calls – they reach out to taxpayers by mail.
- Also educate yourself about your bank or your credit issuers business practices. There are questions they would never ask that scammers will.

Phish-tales – the telltale signs that something might be amiss:

- *Personal Information Requests* - You are asked for things like passwords, mother's maiden name, date of birth, etc.
- *Too Good To Be True* - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems too good to be true, it probably is!
- *Sense of Urgency* - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them.



Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.

- *Hyperlinks* - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different, or it could be a

→

Cyber-Savvy Seniors

Content brought to you by:

Senior Housing Crime Prevention Foundation

&

BROADWAY BANK

Phlushing Phish

continued from page 1

popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.

- *Attachments* - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses.
- *Unusual Sender* – A message might come from a company claiming you've done business with them when you know you haven't. Or a message to you might be missing your name, misspelling it, or uses bad grammar or what might sound like computer translations from another language. Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!

Wear your lifejacket: some phishing scams are quite convincing, so be wary and protect yourself.

- Ensure that your computer security and virus protection is updated and that you have a backup of all of your important files and information – an external hard drive storage device is good for this.
- Make use of multi-factor authentication when available– that is a second step to verify who you are, like a code texted to your phone.
- If you believe any of your passwords have been compromised, change them immediately and don't use them for any other accounts. It is a good practice to use complicated passwords and update them frequently.

The Phishing Report

You can forward phishing emails to spam@uce.gov and reportphishing@apwg.org as well as report problems to the FTC at ftc.gov/complaint. More info available at ftc.gov/phishing