DIGITAL SCAM PROTECTION SAFETY GUIDE

PALMETTO CONNECT

4 COMMON SCAM TACTICS

AND THE WARNING SIGNS TO LOOK OUT FOR

01

PHISHING SCAMS

An email or texting scam designed to get you to share personal information. Scammers will use phishing attacks to trick the recipient into revealing personal financial information, credentials for system logins or other sensitive information.

SIGNS TO SPOT A PHISHING EMAIL

Wording in the subject line that creates a sense of urgency that action needs to be taken immediately.

Unfamiliar addresses

From: Mercury Bank (mercurybank@yahoo.com)

Subject: Urgent, Action Required!

10:10:26 AM (27 minutes ago)

MERCURY BANK

Dear Valued Customer,

Due to recent activities on your account, we have placed a temporary suspension until you verifi your account. Your account will be closed within 24 hours if you do not verifi your account immediatly. If you would like more information on your account Click Here.
Verify your account now by logging in at: https://www.mercurybank.account.com.

Please do not respond to this message. If you would like to contact us, please log in to Mercury Online Banking and send a message to Customer Service.
Mercury Online Banking

bit.ly/t7DTg92

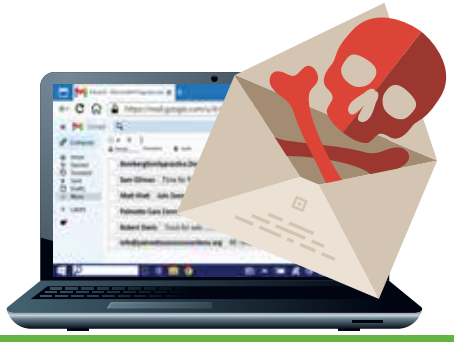
Suspicious links that do not match the destination. To find this information, move your cursor over the link to see the URL.

Noticeable mistakes in spelling or grammar.

Generic greetings or salutations, instead of your real name.

Threats of consequences if you do not respond immediately.

To make emails appear authentic, scammers may even include the logo of a business, but many times the logo will appear fuzzy or colors may not be quite right.



QUISHING SCAMS

02

This is a type of phishing scam, but instead of using email, scammers use QR codes. When these codes are scanned, they can lead you to fraudulent websites or prompt you to download harmful software that will put your personal information at risk. QR stands for “Quick Response.”

7 rules to help you avoid QR code scams.

1. Don't open links or scan QR codes from strangers.
2. Check the link and the destination. To do this, check the link that will appear after you scan the QR code. Scammers will alter addresses in subtle ways such as: rather than the legitimate fedex.com, the URL may appear as: fed-exdelivery.com, or the URL may be completely different.
3. Clicking on shortened links. Shortened links may come from unsolicited communications or even from friends or family if their device has been hacked.
4. Watch out for tampering of a flyer or ads. Scammers have been known to stick their own QR codes over legitimate ones.
5. Stick with your phone's native QR code reader. Steer clear of QR code reading apps. They can be a security risk.
6. Don't pay bills with QR codes. You can't always be sure that the code will send you to a legit site so use a trusted website or another form of payment.
7. Use Text Scam Detector on your phone. This product can be found in the McAfee+ products and can be used as a second line of defense if you accidentally follow as scam link.

03

SMISHING SCAMS

This practice uses text messages or other common messaging apps to trick the person into revealing personal or confidential information. The messages may appear like they are from a reputable company or organization, but they are actually from criminals who want to steal your identity, money, or data.

6 RED FLAGS TO WATCH FOR:

1. Check for numbers you don’t recognize or that are unknown to you.
2. If the message claims to be from a government agency, it is most likely a scam. According to the FCC, they do not initiate contact this way.
3. If you suspect a message is a scam, do not reply, even if it requests that you text “STOP” to end messages. Instead, delete or block the number.
4. Remember, if you didn’t enter a contest and it sounds too good to be true, then it usually is!
5. Watch out for messages asking you to click on a link to log into an account or verify any personal information.
6. Remember the best practice is to go to the official website of the business to log in or to submit any personal data.

Examples of Text Scams

BUSINESS SCAMS

2:00 100%

◄ (803) 278-5546

The Toll Roads Notice of Toll Evasion: You have an unpaid toll bill on your account. To avoid late fees, pay within 12 hours or the late fees will be increased and reported to the DMV https://thetollroads-paytolltre.world/us (Please reply Y, then exit the text message and open it again to activate the link, or copy the link to your Safari browser and open it.)

UPDATE PERSONAL INFO

2:00 100%

◄ Unknown Number

Netflix: We are unable to process your latest bill. In order to avoid any disruption in service, please update your payment information here. https://www.netflix.com/89TyjxdRB978.com

DELIVERY SCAMS

2:00 100%

◄ (888) 452-2121

[ALERT] We attempted to deliver your package today but no one was available. Reply to this message to set up a new delivery date or if you think you have recieved this message in error just text ”STOP” to end messages.

PRIZE SCAMS

2:00 100%

◄ Unknown Number

Congrats Kattie! Your entry last month was selected as the winner of a $1000 Amazon gift card promotion. Click here to claim your prize! https://amazon/claimprize/winner.com

VISHING SCAMS

04

REMEMBER
CALL,
DON'T CLICK

This is a phone scam designed to get you to share personal information. Scammers use voice calls or voicemails to obtain sensitive information. These calls usually have a sense of urgency along with a threat of something severe if the recipient doesn't comply immediately.

Callers or messages asking you to download a file or some other software program to fix a problem.

Some callers may ask you to resolve the issue in question by making instant cash transfers or even buying bulk gift cards, like iTunes.

Unexpected phone calls from someone claiming to be from a government agency, or a well-known financial institution. They may ask you to verify personal information, like a bank account number, Social Security number or even your credit card number.

Callers becoming increasingly aggressive or threateningif you do not comply with their request. They may insist that action has to be taken immediately to avoid being arrested, having your Social Security number cancelled or even having you deported.

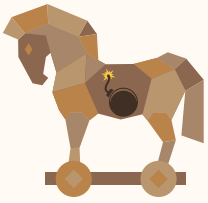
Calls may show up as unknown or other numbers you do not recognize. In some cases, they may even appear to be local numbers. The caller may also have a foreign accent or speaks with poor English, which could be a sign that they are not who they claim to be.

It is important that you understand if you have any doubt or recognize any of these signs, do not disclose personal information or make payments over the phone. Instead, hang up and contact the company or government agency directly using a phone number that you trust.

What is a Virus?

A computer virus is a malicious set of codes meant to gain access to or harm your computer. Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage.

TYPES OF VIRUSES

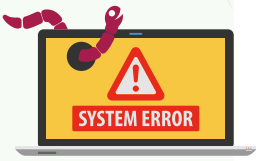


TROJAN HORSE

A program that can be downloaded and installed on your digital device that may appear harmless but is actually a virus.

WORM

Uses your processing power and internet for corrupt purposes.



RANSONWARE

A type of malware that holds your personal files hostage until a "ransom" is paid.

SPYWARE

Records your keyboard strokes thereby stealing private information such as passwords, credit card numbers, etc.

MALWARE

Causes your computer to malfunction, crash, and become non-responsive.

DEFEND YOUR DEVICES
WITH PROVEN ANTIVIRUS SOFTWARE PROGRAMS.

Antivirus software works by scanning your devices regularly to look for and block known viruses and malware. If your device gets infected, antivirus software will help you remove it to provide the best possible protection for your devices and personal data.

FREE ANTIVIRUS SOFTWARE

- Windows Defender
- panda
- AVG

SUBSCRIPTION ANTIVIRUS SOFTWARE

- KASPERSKY lab Internet Security
- Bitdefender
- Norton by Symantec
- McAfee

STOP SCAMMERS & TAKE CONTROL!

Create strong passwords for accounts that you have to log into, such as emails, bank accounts, Amazon accounts or other personal accounts.

- ☑ A strong password consists of at least eight characters
- ☑ Use at least one special character, such as !, @, #, $, *
- ☑ Use at least one number
- ☑ Use a mix of uppercase and lowercase letters

Passwords need to be familiar to you but not something too obvious, so it can't be figured out easily.

SAMPLE PASSWORDS

A favorite food + Mom's birth year
Mix in 2 Special Character
PeachEs(1945*

Number of Children
+ A Special Character + Favorite Color
3!PurPle

ADDITIONAL TIPS
FOR PROTECTION AGAINST SCAMMERS

- If you receive a questionable call, **hang up and report it.**
- Do not return call to unknown numbers.
- Ask for advice from someone you trust before making any large purchases or financial decisions.
- Monitor financial and personal information.
- Update passwords frequently.
- Don't click on pop-ups.

REPORT SCAMS:

SC Department of Consumer Affairs
(844) 835 - 5322 (toll free in SC)
(803) 734 - 4200
consumer.sc.gov

Federal Communications Commission
(888) 225 - 5322
consumercomplaints.fcc.gov

Federal Trade Commission
(877) 382 - 4357
ftc.gov/complaint

STOP SOLICITOR CALLS

If you do not want to receive telemarketing calls you can add your number to the
DO NOT CALL REGISTRY
at: Donotcall.gov or
call (888)382 - 1222

STOP UNSOLICITED OFFERS

Opt out of snail mail marketing
Dmachoice.org

Opt out of pre-approved credit offers:
www.optoutprescreen.com
or call (888)567-8688

PALMETTO CONNECT

1880 Main Highway | Bamberg, SC 29003
803.245.2672
www.palmettocareconnections.org