DON'T BE A VICTIM

SCAMS, FRAUDS, AND SWINDLES: EMAIL PHISHING

In 2020 the Chesterfield Police Department investigated 45 reports concerning scams and frauds totaling over $1.5 MILLION in losses

The following slides discuss one of the many scams Chesterfield residents have fallen victim to

This episode:
Email Phishing

EMAIL PHISHING

- IN THIS SCAM, THE SUSPECTS USE EMAIL OR TEXT MESSAGES TO TRICK A VICTIM INTO GIVING THEM PERSONAL INFORMATION
- THEY WILL USUALLY MAKE THEIR MESSAGE LOOK LIKE THEY ARE FROM A COMPANY YOU KNOW OR TRUST
- THEY WILL TELL A STORY, OR TRICK YOU INTO OPENING A LINK OR ATTACHMENT
- EXAMPLES OF THIS:
  *AN EMAIL SAYING THEY HAVE NOTICED SUSPICIOUS ACTIVITY OR LOG-IN ATTEMPTS
  *CLAIM THERE IS A PROBLEM WITH YOUR ACCOUNT OR PAYMENT INFORMATION
  *SAY YOU MUST CONFIRM PERSONAL INFORMATION
  *THEY WANT YOU TO CLICK ON A LINK TO MAKE PAYMENT/ CHANGE YOUR LOG-IN INFORMATION, UPDATE PERSONAL INFORMATION, ETC.
- THEY MAY CLAIM YOU HAVE “WON A PRIZE” AND TO “CLICK HERE” IN ORDER TO CLAIM IT

EMAIL PHISHING

- IF THE SUSPECT IS ABLE TO CONVINCE YOU TO GIVE THEM YOUR INFORMATION, THEY CAN GAIN ACCESS TO YOUR EMAIL, BANK ACCOUNTS, OR MANY OTHER TYPES OF ACCOUNTS
- THEY CAN INFECT YOUR DEVICE WITH MALWARE
- THEY CAN CAUSE EXTREME FINANCIAL LOSS AND FRUSTRATION AS YOU TRY TO FIX THE DAMAGE

EMAIL PHISHING

THINGS TO LOOK FOR:

- **SENSE OF URGENCY** – A FAVORITE TACTIC IS TO MAKE YOU ACT FAST BECAUSE OF TIME LIMITS
- **HYPERLINKS** – A LINK MAY NOT BE ALL IT APPEARS TO BE. HOVER OVER THE LINK WITH YOUR MOUSE TO SEE WHERE YOU WILL ACTUALLY BE DIRECTED UPON CLICKING IT.
- **ATTACHMENTS** – IF YOU SEE AN ATTACHMENT IN AN EMAIL YOU WEREN'T EXPECTING OR IT DOESN'T MAKE SENSE , DON'T OPEN IT
- **UNUSUAL SENDER** – WHETHER IT LOOKS LIKE SOMEONE YOU KNOW, OR DON'T KNOW, IF ANYTHING SEEMS OUT OF THE ORDINARY/ UNEXPECTED/ OUT OF CHARACTER/ SUSPICIOUS – DON'T CLICK ON IT
- **IF IT SEEMS TOO GOOD TO BE TRUE, IT PROBABLY IS**

EMAIL PHISHING

HOW TO PROTECT YOURSELF:

- KEEP YOUR SECURITY SOFTWARE UP TO DATE
- PROTECT YOUR ACCOUNTS BY USING MULTI-FACTOR AUTHENTICATION: BACK UP YOUR DATA
- LOOK FOR CLUES IN THE MESSAGE – POOR ENGLISH, MISSPELLINGS, USING A GENERIC GREETING INSTEAD OF YOUR NAME, STRANGE/UNEXPECTED SOLICITATION THAT SEEMS “OFF”
- FOR FURTHER CLICK ON THIS LINK : HOW TO RECOGNIZE AND AVOID PHISHING SCAMS

EMAIL PHISHING

HOW TO PROTECT YOURSELF (CONTINUED)

- NO LEGITIMATE BUSINESS WILL SEND YOU UNSOLICITED ATTACHMENTS TO OPEN
- IF YOU ARE NOT SURE, CONTACT THE BUSINESS WHO ALLEGEDLY SENT YOU THE EMAIL BY USING THE BUSINESS INFORMATION FROM THEIR LEGITIMATE WEBSITE, NOT THE CONTACT INFORMATION ON THE SUSPICIOUS EMAIL
- CONTACT YOUR LOCAL POLICE DEPARTMENT
- REPORT THE ELECTRONIC SCAM TO IDENTITYTHEFT.GOV
- BOTTOM LINE- DON'T OPEN ATTACHMENTS UNLESS YOU ARE EXPECTING THEM. DON'T GIVE OUT ANY PERSONAL INFORMATION UNLESS YOU ARE SURE WHO YOU ARE COMMUNICATING WITH. BE VIGILANT