Scammer and Spammer Fraud

How to recognize and avoid internet, telephone, and mail scams for your personal and church finances

Ministry and Mission Day
Presented by the Commission on Stewardship
Presenters: Zach Tabor and Doug Harrison
May 7, 2022

[2]

Thank you for attending this workshop dedicated to educating you on different types of scams that can affect your personal finances, the finances of your loved ones, the finances of your church, and even your identity. We hope that after the presentation you will have a better knowledge of what these scams look like so that you can avoid them and help others see these scams before they fall prey to them as well. Most importantly, we want everyone to open up about being scammed and seeing these scams so that we can protect each other.

What is the difference between Spam and Scam?

Everyone has gotten an email advertising something they were not searching for and phone calls telling them about better business supplies, car extended warranties, and mortgage options that you have to act on immediately so you don't miss out. These are all examples of spam. The word "spam" is thought to come from a sketch on Monty Python's Flying Circus, a British comedy and satire series, that featured a couple in a restaurant trying to choose their dinner but instead found that every meal contained spam meat. Spam is flooding the internet with the same message sent to millions of people at a time with no specific target. The majority of spam is commercial advertising for products that might seem rather suspicious. Spammers want you to buy their dubious wares, access their dubious sites, or just forward their messages to others. Clicking on spam emails or advertisements or agreeing to anything in a spam call usually leads to buyer's remorse and annoyance, but there are no serious financial issues to follow.

A scam, whether it be some sort of phishing email or phone call or someone presenting themselves fraudulently, is meant to get information from you so that your finances and/or identity can be accessed and used for a fraudster's financial benefit. Scams usually start with a notice that you have won a prize, you have made a purchase that you actually haven't, or a greeting for further engagements, either friendly or romantic. The result is always the stealing of your information.

This presentation will focus on phishing schemes, romance scams, and grandparents' scams. We will also cover ways to spot these scams and how to avoid them.

Phishing Schemes

Phishing emails and phone calls want your information: your usernames, your passwords, credit card details, etc. Phishing emails also will be familiar to you in one respect or another. The email or call may represent itself as your credit card company, an organization to which you have donated, or even the IRS! Let's go over the types of phishing emails/phone calls that you can encounter.

Deceptive Phishing Emails

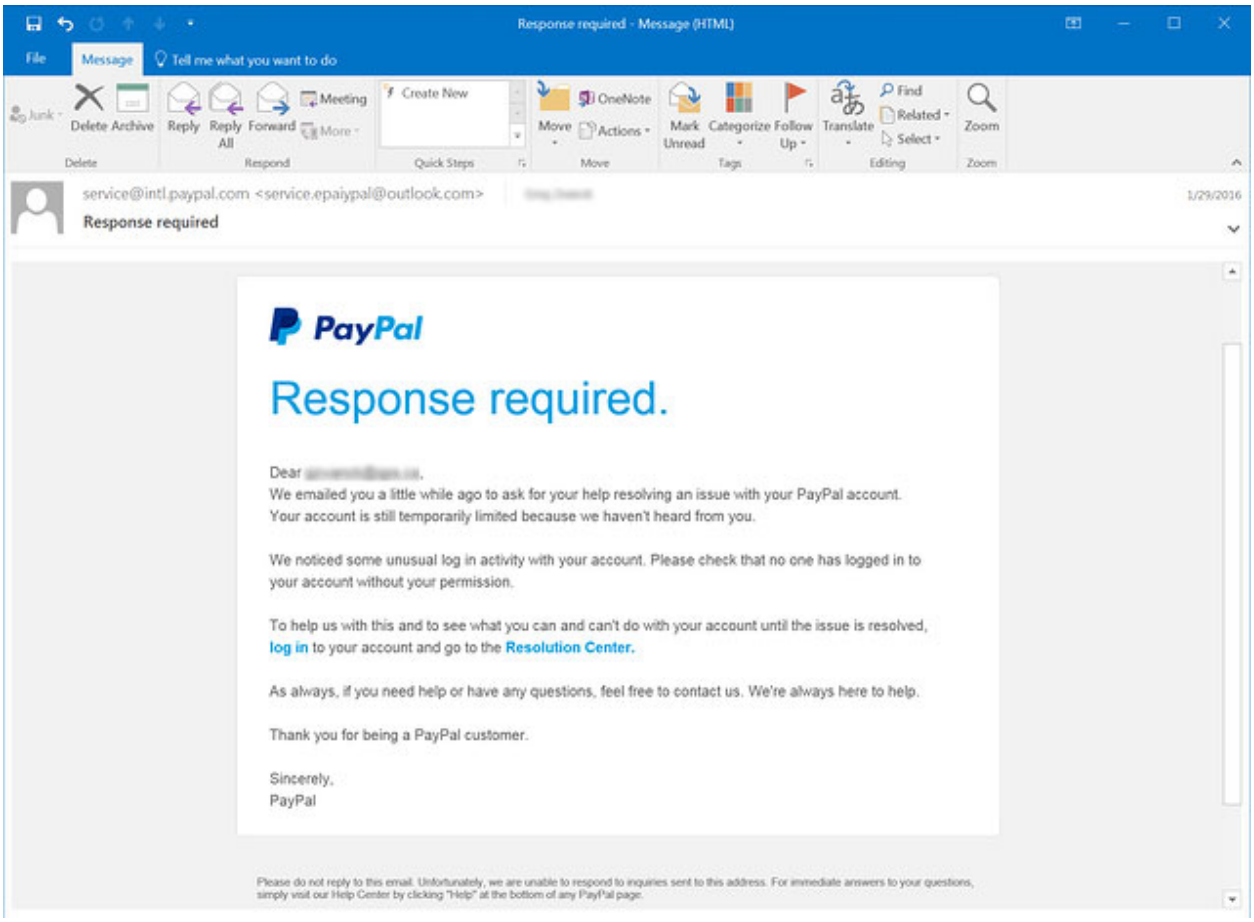
Deceptive phishing is the most common type of phishing scam. In this ploy, fraudsters impersonate a legitimate company to steal people's personal data or login credentials. Those emails use threats and a sense of urgency to scare users into doing what the attackers want.

Techniques Used in Deceptive Phishing Emails

- Legitimate links – Many attackers attempt to evade detection from email filters by incorporating legitimate links into their deceptive phishing emails. They could do this by including contact information for an organization that they might be spoofing.
- Blend malicious and benign code – Those responsible for creating phishing landing pages commonly blend malicious and benign code together to fool Exchange Online Protection (EOP). This might take the form of replicating the CSS and JavaScript of a tech giant's login page to steal users' account credentials.
- Redirects and shortened links – Malicious actors don't want to raise any red flags with their victims. They therefore use shortened URLs to fool Secure Email Gateways (SEGs). They also use "time bombing" to redirect users to a phishing landing page only after the email has been delivered. After victims have forfeited their credentials, the campaign then redirects victims to a legitimate web page.
- Modify brand logos – Some email filters can spot when malicious actors steal organizations' logos and incorporate them into their attack emails or onto their phishing landing pages. They do so by looking out for the logos' HTML attributes. To fool these detection tools, malicious actors alter an HTML attribute of the logo such as its color.

- Minimal email content – Digital attackers attempt to evade detection by including minimal content in their attack emails. They might elect to do this by including an image instead of text, for instance.

Example of a Phishing Email



- First, notice that this email is supposed to be from PayPal, but the email address has the server address "@outlook.com". PayPal would have their own email server and would not use the public extension for Outlook/Microsoft email users.
- The email wants you to resolve a login issue. The first thing you should do is login to your PayPal account on your web browser and not through the links in the email. If you can log in with no issue, then you have confirmed this is a fraudulent phishing email.
- Finally, notice the lowercase "r" in "required" that proceeds the capitalized "R" in "Response". As this is a title, both words need to be capitalized. This may seem minor, but you should always read the email carefully and look for grammar, syntax, and spelling errors.

How to Defend Against Deceptive Phishing Emails

- The success of a deceptive phish hinges on to what extent an attack email resembles official correspondence from a spoofed company. Acknowledging that fact, users should inspect all URLs carefully to see if they redirect to an unknown and/or suspicious website.
- As stated before in the example, look out for generic salutations, grammar mistakes, and spelling errors.
- NEVER click links in an email that you find suspicious. Always navigate to your login through your web browser as you normally do.
- Call the company that you received the email from by using your number on file for the company or by searching the company's number through Google, Bing, DuckDuckGo, etc.
- If you call the number given in an email, NEVER allow them to connect to your computer. In the case of an email confirming a purchase that you never made, any legitimate emails can be made back to your bank or the credit card company. NEVER allow anyone to access your computer or your online banking portal.

Vishing, Phone Calls Fishing for Your Information

This type of phishing attack dispenses with sending out an email and goes for placing a phone call instead. As noted by Comparitech, an attacker can perpetrate a vishing campaign by setting up a Voice over Internet Protocol (VoIP) server to mimic various entities in order to steal sensitive data and/or funds. Malicious actors used those tactics to step up their vishing efforts and target remote workers in 2020, found the FBI.

Techniques Used in Vishing

- "The mumble technique": Digital attackers will oftentimes incorporate unique tactics to go after specific targets. For instance, as reported by Social-Engineer, LLC, when they attempt to target customer service representatives or call center agents, malicious actors might use what's known as "the mumble technique" to mumble a response to a question in the hopes that their "answer" will suffice.
- Technical jargon: If malicious actors are targeting a company's employees, Social-Engineer, LLC noted that they might impersonate in-house tech support by using technical jargon and alluding to things like

speed issues or badging to convince an employee that it's okay for them to hand over their information.
- ID spoofing: Here, a malicious actor disguises their phone number to make their call look like it's coming from a legitimate phone number in the target's area code. This technique could lull targets into a false sense of security.

Example of Vishing, the IRS Scam

You have probably once, if not a thousand times, gotten a call from the Internal Revenue Service telling you that you owe money to the federal government. This call will include a large amount that needs to be paid immediately. The call, which is usually done by a robocall or dialer, will also tell you than the local police have been notified and will come to send you to jail if the money is paid in a specific amount of time.

First of all, the IRS will never call you. Just try calling the IRS and see how long it takes to get an actual person to talk to you. But let's say you do stay on the line or your hit the prompt given in the call to talk to someone about this tax liability that you have to pay. Chances are you will talk to someone that will first bring down the amount you owe. You will need to pay them with cash that you mail or with prepaid store or debit cards. This payment is needed by the scammer because they need something that cannot be traced. This should be your ultimate clue that this person is trying to scam you. Hang up or keep messing with them until they hand up on you.

Smishing, Text Messages Fishing for Your Information

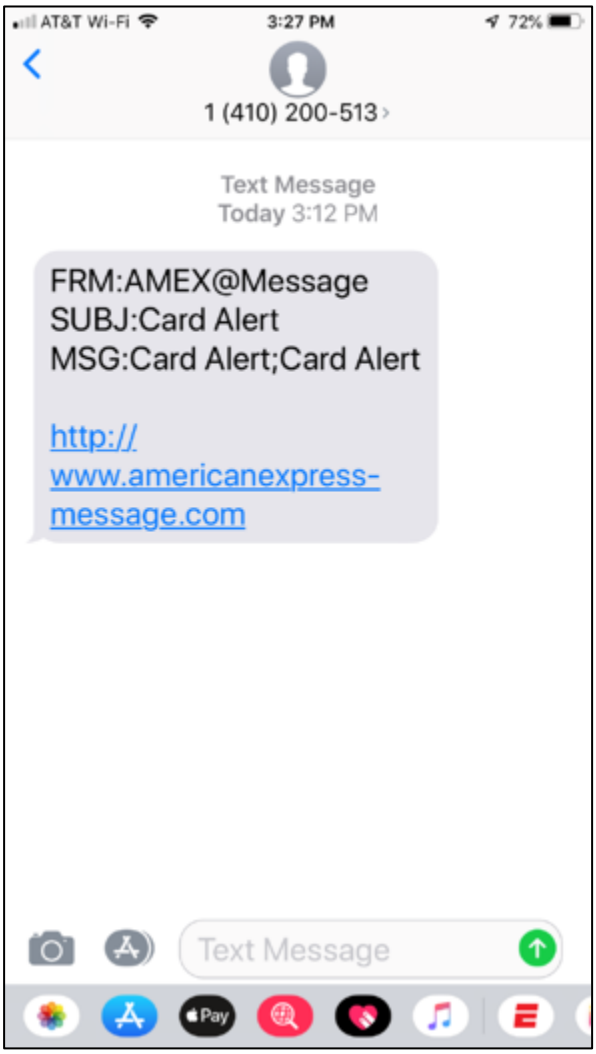
Vishing isn't the only type of phishing that digital fraudsters can perpetrate using a phone. They can also conduct what's known as smishing. This method leverages malicious text messages to trick users into clicking on a malicious link or handing over personal information.

Techniques Used in Smishing

- Trigger the download of a malicious app: Attackers can use malicious links to trigger the automatic download of malicious apps on victims' mobile devices. Those apps could then deploy ransomware or enable nefarious actors to remotely control their devices.

- Link to data-stealing forms: Attackers could leverage a text message along with deceptive phishing techniques to trick users into clicking a malicious link. The campaign could then redirect them to a website designed to steal their personal information.
- Instruct the user to contact tech support: With this type of attack tactic, malicious actors send out text messages that instruct recipients to contact a number for customer support. The scammer will then masquerade as a legitimate customer service representative and attempt to trick the victim into handing over their personal data.

Example of Smishing



[8]

How to Defend Against Smishing

Users can help defend against smishing attacks by researching unknown phone numbers and by calling the company named in suspicious SMS messages if they have any doubts. Many of the techniques given above to Phishing Emails can be used to verify SMS and MMS text messages that you receive on your phone.

Romance Scams

Adults of all ages are going online in hopes of finding love and companionship. Worldwide, 1 in 5 people ages 45 to 54 and 1 in 7 ages 55 to 64 have used a dating website or app, according to a 2021 survey by data firm Statista.

But seeking romantic bliss online can have a major downside: Cyberspace is full of scammers eager to take advantage of lonely hearts, and their ranks are growing. The Federal Trade Commission (FTC) received some 56,000 complaints about romance scams in 2021, more than triple the 2017 total, and reported monetary losses from such cons jumped sixfold over the same period, to $547 million.

The con typically works something like this: You post a dating profile and up pops a promising match — good-looking, smart, funny and personable. Supposed suitors might also reach out on social media; more than a third of people who lost money to a romance scam in 2021 reported that it started on Facebook or Instagram, according to the FTC.

This potential mate claims to live in another part of the country or to be abroad for business or a military deployment. But he or she seems smitten and eager to get to know you better, and suggests you move your relationship to a private channel like email or a chat app.

Over weeks or months, you feel yourself growing closer. You make plans to meet in person, but for your new love something always comes up. Then you get an urgent request. There's an emergency (a medical problem, perhaps, or a business crisis) and your online companion needs you to send money fast, usually via gift cards, prepaid debit cards, cryptocurrency, or a bank or wire transfer.

They'll promise to pay it back, but that will never happen. Instead, they will keep asking for more until you realize it's a scam and cut them off.

Romance scams can overlap with or evolve into other forms of fraud. For example, international criminal gangs use dating sites to recruit unwitting "money mules" to launder ill-gotten funds through their bank accounts or other means. And con artists are increasingly luring supposed sweethearts into fraudulent cryptocurrency investments.

The older the target, the heavier the financial toll. The median individual loss from a romance scam for people 70 and over was $9,000 in 2021, according to the FTC, compared to $2,400 across all age groups.

[Source: AARP Website]

How to Defend Against Romance Scams

- Protect yourself and older loved ones by raising awareness. Although this can be an uncomfortable topic, make sure you, your family and your friends are familiar with romance scams. The more you know about these scams, the better prepared you are to prevent being a victim.
- Check in on older loved ones. Scammers are seeking to target those living alone or grieving the loss of a spouse as they are more vulnerable.
- Limit what you share online. Scammers can use details shared on social media and dating sites to better understand and target you.
- Do your research. Research the individual's photo and profile using online searches to see if the image, name or other details have been used elsewhere.
- Go slowly and ask lots of questions. Don't let the individual rush you to leave a dating service or social media site to communicate directly.
- Listen to your gut. If the individual seems too good to be true, talk to someone you trust.
- Don't overshare personal information. Requests for inappropriate photos or financial information could later be used to extort you.
- Be suspicious if you haven't met in person. If the individual promises to meet in person, but consistently comes up with an excuse for cancelling, be suspicious.
- Don't send money. Never send money to anyone you have only communicated with online or by phone.

Grandparent Scams

Grandparents often have a hard time saying no to their grandchildren, which is something scam artists know all too well.

Scammers who gain access to consumers' personal information – by mining social media or purchasing data from cyber thieves – are creating storylines to prey on the fears of grandparents. The scammers then call and impersonate a grandchild in a crisis situation, asking for immediate financial assistance. The callers may "spoof" the caller ID that appears on the recipient's phone to make an incoming call look like it's coming from a trusted source.

Example of a Grandparent Scam

In a recent report from the FBI in Buffalo, N.Y., a caller contacted an elderly person in western New York state and claimed to be a grandchild who had just been in a serious car accident and arrested for drunk driving. The imposter pressed the grandparent for money to post bond, then passed the phone to someone else who claimed to be the caller's attorney.

That phony attorney told the grandparent to come up with approximately $15,000 in cash and to put it in an envelope to be picked up at their house by a courier at a designated time. When the courier arrived, the unsuspecting grandparent handed over the cash. The FBI reports that these scams may use ride-share companies to retrieve the cash from victims.

Several variations of this con have surfaced over the years. The U.S. Postal Inspection Service recently published an article about grandparent scams, with videos of victims sharing their stories to help raise awareness of this criminal tactic.

[Source: FCC Website, 05/25/2021]

How to Defend Against Grandparent Scams

- The best advice for avoiding this type of scam, or any suspicious phone call, is to hang up immediately. If you have caller ID and you don't recognize an incoming phone number, just let it go to voicemail.

- If you do wind up in a conversation, use caution if you are being pressured for information or to send money quickly. Scammers often try to bully victims into transferring money through a mobile payment app, by wiring money, or by purchasing gift cards or money orders. If you receive a call like this, report it immediately to local law enforcement.

Final Comments and Tips to Prevent Scams

For yourself, your loved ones, and your church, please consider the following suggestions to help prevent scammers from taking advantage of you:

- If you are not familiar with a phone number (voice and text) or an email address, do not answer and do not open the message.
- Make sure to keep track of your usernames and passwords and not to rely on applications to remember them for you. Even though it is convenient to keep your usernames and passwords saved on websites and apps on your phone, anyone that gains access to your computer and/or phone will also have your credentials.
- Consider using a credit card for your purchases instead of a debit card issued through your bank. Using a credit card through a third-party credit service (Chase, American Express, Discover, etc.) allows for far greater liability protection than a debit card through your bank. Charges that you question on your credit card require the burden of proof from the credit bureau than you made the purchase. Any charges that you did not make can easily be taken off your account and a new card issued. A debit card through a bank however requires you to prove you did not make a purchase. Cases for fraud are long with banks and it is much harder to prove and get your money back from the bank.
- Do not have any shame in being scammed. It happens to all of us and keeping it secret only hurts you and everyone you know. The more we talk about these issues without shame or contempt will allow us all to be more informed and better protected in spotting these scams in the future.
- Anything that seems too good to be true is probably a scam when it comes to finances and romantic adventures.

Resources for Phishing and Other Scam Prevention and Awareness

Federal Communications Commission
https://consumercomplaints.fcc.gov/

Federal Trade Commission
https://reportfraud.ftc.gov/
Phone: 1-866-347-2423

USA.gov Resources
https://www.usa.gov/federal-agencies
https://www.usa.gov/state-consumer

National Center for Disaster Fraud
https://www.justice.gov/disaster-fraud/webform/ncdf-disaster-complaint-form
Phone: 1-866-720-5721

Federal Bureau of Investigation
https://www.fbi.gov/scams-and-safety