Scams and Keeping Safe

MG Computer Club Presentation 11/10/20

Scams

Telephone Scams

Telephone scammers try to steal your money or personal information. Scams may come through phone calls from real people, robocalls, or text messages. The callers often make false promises, such as opportunities to buy products, invest your money, or receive free product trials. They may also offer you money through free grants and lotteries. Some scammers may call with threats of jail or lawsuits if you don't pay them.

Report Telephone Scams

- Reporting scams to federal agencies helps them collect evidence for lawsuits against people committing these scams. However, federal agencies don't investigate individual cases of telephone scams.
- Report telephone scams to the Federal Trade Commission, either online or by phone at 1-877-382-4357. This is the primary government agency that collects scam complaints.
- Report all robocalls and unwanted telemarketing calls to the Do Not Call Registry.
- Report caller ID spoofing to the Federal Communications Commission either online or by phone at 1-888-225-5322.
- Also report the scam to your state consumer protection office. Some consumer protection offices help residents resolve consumer problems.

How to Protect Yourself

Remember these tips to avoid being a victim of a telephone scam:

Do

- Register your phone number with the National Do Not Call Registry. You may register online or by calling 1-888-382-1222. If you still receive telemarketing calls after registering, there's a good chance that the calls are scams.
- Be wary of callers claiming that you've won a prize or vacation package.
- Hang up on suspicious phone calls.
- Be cautious of caller ID. Scammers can change the phone number that shows up on your caller ID screen. This is called "spoofing."
- Research business opportunities, charities, or travel packages separately from the information the caller has provided.

Don't

- Don't give in to pressure to take immediate action.
- Don't say anything if a caller starts the call asking, "Can you hear me?" This is a common tactic for scammers to record you saying "yes." Scammers record your "yes" response to use as proof that you agreed to a purchase or credit card charge.
- Don't provide your credit card number, bank account information, or other personal information to a caller.
- Don't send money if the caller tells you to wire money or pay with a prepaid debit card.

Banking Scams

Banking scams involve attempts to access your bank account. Some popular banking scams include:

- Overpayment scams - A scam artist sends you a counterfeit check. They tell you to deposit it in your bank account, and wire part of the money back to them. Since the check was fake, you'll have to pay your bank the amount of the check, plus you'll lose any money you wired.
- Unsolicited check fraud - A scammer sends you a check for no reason. If you cash it, you may be authorizing the purchase of items or signing up for a loan you didn't ask for.
- Automatic withdrawals - A company sets up an automatic debit from your bank account, as part of a free trial or to collect lottery winnings.
- Phishing - You receive an email message that asks you to verify your bank account or debit card number.
- Report Banking Scams
- The proper organization to report a banking scam to depends on which type you were a victim of.

- Report fake checks you receive by mail to the US Postal Inspection Service.
- Report counterfeit checks to the Federal Trade Commission, either online or by phone at 1-877-382-4357.
- Contact your bank to report and stop unauthorized automatic withdrawals from your account.
- Forward phishing emails to the Federal Trade Commission at spam@uce.gov.

How to Protect Yourself

Remember these tips to avoid being a victim of a banking scam:

Do

- Be suspicious if you are told to wire a portion of funds from a check you received back to a company.
- Be wary of lotteries or free trials that ask for your bank account number.
- Verify the authenticity of a cashier's check with the bank that it is drawn on before depositing a check.
- When verifying a check or the issuer, use contact information on a bank's website.

Don't

- Don't trust the appearance of checks or money orders. Scammers can make them look legitimate and official.
- Don't deposit checks or money orders from strangers or companies you don't have a relationship with.
- Don't wire money to people or companies you don't know.
- Don't give your bank account number to someone who calls you, even for verification purposes.
- Don't click on links in an email to verify your bank account.
- Don't accept a check that includes an overpayment

Charity Scams

Some scammers set up fake organizations, to take advantage of the public's generosity. They especially take advantage of tragedies and disasters.

Report Charity Scams

- Your state consumer protection office can accept and investigate consumer complaints.
- File a complaint with the Federal Trade Commission (FTC). The FTC does not resolve individual matters. But it does track charity fraud claims and sues companies on the behalf of consumers.
- Contact the National Center for Disaster Fraud, if the suspected fraud is because of a natural disaster.
- The Do Not Call Registry doesn't apply to charities. But you can ask an organization not to contact you again.

How to Protect Yourself

Follow these tips to help you detect common charity scam tactics:

Do

- Check out the charity with your state consumer protection office or the Better Business Bureau before you give.
- Verify the name. Fake charities often choose names that are close to well established charities.

Don't

- Don't give in to high pressure tactics such as urging you to donate immediately.
- Don't assume that you can get a tax deduction for donating to an organization. Use the IRS's database of 501(c)3 organizations to find out if it has this status.
- Don't send cash. Pay with a check or credit card.

Ticket Scams

Ticket selling scams happen when a scammer uses tickets as bait to steal your money. The scammer usually sells fake tickets or you pay for a ticket, but never receive it. They are common when tickets for popular concerts, plays, and sporting events sell out. Scammers, including individuals and fake resale companies, take advantage of the situation by:

- Charging prices much higher than the face value of a ticket
- Creating counterfeit tickets with forged barcodes and logos of real ticket companies
- Selling duplicates of a legitimate ticket and emailing it to several buyers.
- Pretending to sell tickets online to steal your credit card information

Report ticket scams

There are several options to report a ticket scam.

- Contact your state consumer protection office.
- Contact the Federal Trade Commission (FTC) using the Online Complaint Assistant.
- File a local police report, especially if you met the scammer in person or have a picture of them to give the police.
- Report it using the Better Business Bureau's Scam Tracker.
- If you paid by credit card, report the problem to the card company. You may be able to dispute the charge.

- How to protect yourself
- Learn what you can do to avoid becoming a victim:

Do

- Buy tickets at the venue box office.
- Buy tickets from authorized brokers and third party sellers, with verified contact information.
- Verify that the seller has a real physical addresses and phone numbers. Scammers often post fake addresses, PO Box, or no address on their websites.
- Check the actual web address of the resale ticket seller. Some scammers create phony websites that closely resemble authentic ticket company websites.
- Search for negative reviews about the seller. Use the seller's name, email address, and phone number, along with the words "fraud," "scams," and "fake tickets" for your online search.
- Look at the tickets before you buy and verify the date and the time printed on them.
- Make sure the section and seat numbers on the tickets actually exist at the venue.
- Have the seller meet you in person in a public place for the ticket exchange.
- Ask the seller for proof that they bought the tickets, if you are buying from an individual.
- Use a credit card to pay third party sellers. Your credit card offers protections, if you need to dispute a charge.
- Check for complaints against a ticket seller with your state's consumer protection agency.

Don't

- Don't wire transfer money to pay for tickets.
- Don't trust sellers who want you to pay with a prepaid money card.
- Don't pay before seeing the tickets
- Don't meet an individual ticket seller alone or in a low-traffic area.
- Don't automatically trust online search results for ticket sellers. Search results can include paid ads, sellers that charge high fees, and scams.

Lottery and Sweepstakes Scams

Prize scammers try to get your money or personal information through fake lotteries, sweepstakes, or other contests. Many claim that you've won a prize but must pay a fee to collect it. Others require you to provide personal information to enter a "contest." These scams may reach you by postal mail, email, phone call, robocall, or text message.

State and local laws govern legitimate lotteries and sweepstakes. State lotteries publish their results online or broadcast them on television, not by contacting you directly.

Report Lottery and Sweepstakes Scams

To report a prize scam:

- Contact the Federal Trade Commission online or by phone at 1-877-382-4357.
- Contact a postal inspector if the scam uses U.S. mail to further its scheme. It doesn't matter if the scam notice arrived by phone or email.
- Report robocalls and unwanted telemarketing calls to the Do Not Call Registry.
- Federal agencies investigate scams and pursue criminal charges against the scammers. They don't, however, investigate individual cases. State consumer protection offices might pursue individual cases as well as investigate scams.

How to Protect Yourself

Remember these tips to avoid being a victim of a lottery or sweepstakes scam:

Do

- Check the postage on a mailed prize notice. If it was sent bulk rate, it's probably a scam.
- Try to remember if you entered a particular contest. If you don't remember entering it, the prize notice is likely a fake.
- Some scammers use the names of organizations that run real sweepstakes. Research the company's contact information. Contact them to verify if the prize is legitimate.
- Register your phone number with the National Do Not Call Registry. You may register online or by calling 1-888-382-1222. If you receive telemarketing calls after registering, there's a good chance that the calls are scams.
- Report spam text messages to your mobile carrier, then delete them.
- Hang up on suspicious calls.

Don't

- Don't pay a fee, taxes, or shipping charges to receive a prize.
- Don't wire money to, or deposit a check from, any organization claiming to run a sweepstakes or lottery.
- Don't provide your credit card number or bank account information to receive a prize.
- Don't automatically believe anyone who says they're from the government or an official-sounding organization.
- Don't reply to, or click on any links in, a spam text message.
- Don't attend a sales meeting to be eligible to win a prize.
- Don't give in to pressure to take immediate action.
- Don't believe anyone claiming to be from a foreign lottery or sweepstakes. It's illegal to enter foreign contests like these.

Pyramid Schemes

Pyramid schemes are scams that need a constant flow of new participants to keep them going. They are marketed as multi-level marketing programs or other types of legitimate businesses. They use new recruits' "investments" to pay "profits" to those participating longer.

Pyramid schemes collapse when they can't recruit enough new participants to pay earlier investors. These scams always fail—it's mathematically guaranteed.

Report Pyramid Schemes

Report pyramid schemes to:

- Your state consumer protection office
- The Federal Trade Commission
- How to Protect Yourself

Keep these tips in mind to avoid falling for a pyramid scheme:

Do

- Be wary if you have to recruit more participants to increase your profit, or get your investment back.
- Ask if the company sells non-tangible products or technical services, rather than physical items.

- Check out the business with the Better Business Bureau, your state attorney general, or state licensing agencies.
- Ask to see financial statements audited by a certified public accountant (CPA). Find out if the company earns income from selling its products or services to customers, not to its sales team.
- Be skeptical of success stories and testimonials of fantastic earnings.

Don't

- Don't invest until you've verified that the business is legitimate.
- Don't get involved in businesses that make you recruit new participants.
- Don't buy into franchises that promise big or quick profits.
- Don't invest in any "opportunity" bearing warning signs of a pyramid scheme.
- Investment Scams
- Investment scams prey on your hope to earn high returns on a regular basis, without financial risk.

Report Investment Scams

Report investment scams, if you have been a victim.

- File a complaint about an investment or an investment account with the Securities and Exchange Commission (SEC).
- Report pyramid or Ponzi schemes to the Federal Trade Commission (FTC).
- Report investment scams by state-licensed companies to your state's securities administrator.
- The SEC may forward your complaint to the investment company. It will request that the company reply to your complaint. The FTC will not research your individual case of investment fraud.

How to Protect Yourself

Remember these tips to avoid being a victim of an investment scam:

Do

- Research investment opportunities and investment professionals. Your state securities regulator and the Financial Industry Regulatory Authority. offer information.
- Learn where the investment and the investment professional have registered. It may be in your state or with other regulators.
- Get all the details of an investment in writing, but still do your own research.
- Ask questions about costs, timing, risks, and other issues.

Don't

- Don't give in to pressure to invest immediately.
- Don't be influenced by promises that seem too good to be true. These promises may include "guaranteed earnings" or "risk-free" investments.
- Don't invest in something just because the investment professional is nice, seems trustworthy, or has professional titles.
- Don't invest based on claims that other people, "just like you", have invested.
- Don't feel obligated to invest, even if the professional gave you a gift, lunch, or reduced their fees.

Census Related Fraud

The U.S. Census Bureau collects data about the people and economy of the United States. It collects personal and demographic information from people and businesses.

Some scam artists may pretend to be work for the Census Bureau. They'll try to collect your personal information to use for fraud or to steal your identity. These scam artists may send you letters that seem to come from the U.S. Census Bureau. Others may come to your home to collect information about you.

Report Census Related Fraud

If you suspect fraud, report it to the Census Bureau's regional office for your state. Forward scam emails to the Census Bureau at ois.fraud.reporting@census.gov.

How to Protect Yourself

Follow these tips to ensure that your personal information stays safe:

Do

- Verify that the study is legitimate. Check the survey name on the Census Bureau's list of surveys.
- If someone comes to your home and claims to be a census worker, verify that they work for the Census Bureau.
- Look up the employee's name in the Census staff directory.
- Ask to see their badge. A Census Bureau badge has a picture of the field agent, a Department of Commerce watermark, and an expiration date.
- Follow these tips to help you spot census scams, so you don't become a victim.

Don't

- Don't share your full Social Security number, bank or credit card account numbers, or your mother's maiden name. The Census Bureau won't ask for this type of information.
- Don't trust emails from claiming to be from the Census Bureau. This agency sends letters to invite individuals to take part in its surveys. If you get an email from the Census Bureau, it's probably a scam.
- Don't trust caller ID. Call the Census Bureau's National Processing Center to verify a telephone survey.

Ponzi Schemes

A Ponzi scheme is a type of investment fraud. It relies on money from new investors to pay "returns" to current investors. The scheme organizers need to attract new investors all the time and try to keep current investors from cashing out. When they can't, the scheme collapses.

Report Ponzi Schemes

Report Ponzi schemes to:

- The Securities and Exchange Commission (SEC)
- The Financial Industry Regulatory Authority
- Your state's securities administrator

How to Protect Yourself From Ponzi Schemes

Keep these tips in mind to protect yourself from Ponzi schemes:

Do

- Be wary of any investment that regularly pays positive returns regardless of what the overall market is doing.
- Avoid investments if you don't understand them or can't get complete information about them.
- Be alert to account statement errors, which may be a sign of investment fraud.
- Be suspicious if you don't receive a payment or have difficulty cashing out.

Don't

- Don't put your money in investments that promise big returns with little to no risk.
- Don't contribute to any investment that isn't registered with the SEC or with state regulators.
- Don't get financially involved with any unlicensed investment professional or unregistered firm.

Government Grant Scams

Government grant scammers try to get your money by guaranteeing a free grant to help you pay for college, home repairs, or other expenses. They ask for your checking account information so they can "deposit the grant money into your account" or withdraw a "one-time processing fee."

In reality, the government rarely grants money to individuals. It's generally awarded to state and local governments, universities, and other organizations to pay for research and projects that benefit the public.

Report Grant Scams

- If you think you've been a victim of a government grant scam, report it to the Federal Trade Commission. You can file a complaint with the FTC online, or call toll-free 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters fraud-related complaints into a database available to law enforcement agencies in the U.S. and abroad.
- If you've paid a fee to learn about or apply for a government grant, you can report it to your state consumer protection office. The government does not charge for information or applications for federal grants.

How to Protect Yourself

Remember these tips to avoid being a victim of a grant scam:

Do

- Be wary of advertisements and calls about free government grants. These are usually scams.
- Register your phone number with the National Do Not Call Registry to reduce the number of telemarketing calls you receive. Register online at donotcall.gov or by calling 1-888-382-1222 (TTY: 1-866-290-4236) from the phone number you wish to register.

Don't

- Don't give your bank account information to anyone you don't know.
- Don't pay any money for a government grant. You can get Information about government grants for free at public libraries and online at Grants.gov. Government agencies don't charge processing fees for grants they've awarded.
- Don't believe callers who claim they're from an official-sounding government agency with news about a grant. Check out the name of the agency online or in the phone book—it may be fake.

- Don’t assume a phone call is originating from the area code displayed on your caller ID. Some scam artists use technology to disguise their location and make it appear as if they’re calling from Washington, DC.

Amazon Scams

https://www.freep.com/story/money/personal-finance/susan-tompor/2020/10/12/prime-day-2020-amazon-online-shopping-scams/5966052002/

FTC Current Scams

https://www.consumer.ftc.gov/features/scam-alerts

amazon®

Refund Notification

Dear Customer,

Due to a system error you were double charged for your last order. A refund process was initiated but could not be completed due to errors in your billing information.
You are required to provide us a valid billing address.
Click here to update your billing address.

After your information has been validated you should get your refund within 3 business days.

REFERENCE CODE: 3500AMZG

We hope to see you again soon.
amazon.com

From: Amazon <account-update@amazon-com.[redacted]>
To: [redacted]
Subject: Amazon Account Locked : Confirm Your Identity

---

amazon

Dear Suspended user,

Your Prime Membership Account Has Been Suspended Due To The Following Problems Below.

- Invalid Card Number
- Your Billing Address Does Not Match Our Records
- Unverified Email Address

You will not be able to Buy and Sell on amazon until you have click the link below to confirm your account details before 24hrs of receiving this message.

We will be forced to deactivate your account automatically if you do not verify your identity .

If you wish to deactivate your account permanently, Kindly delete and disregard this message immediately.

Click Here To Verify Account

Fw: [Monthly Statement Added] Confirmation notice: information activity on Wednesday 13 September 2019 #JLQUUUNZ/ Confirmation changer le mot de passe de votre compte JLQUUUNZ- Friday, September 13, 2019

A

account-alert@amazon.com <817r90683mb@xmltmxl.info>
Sat 9/14/2019 12:10 AM
coustumer@live.com

amazon

Customer Support

Hello Dear Customer,

We have faced some problems with your account, So Please update your account details. If you do not update your account within 24 hours (from opening this email) will be officially permanently disabled.

Update Now

We hope to see you again soon.

Amazon.com

Filip

[Ap] Your Apple ID has been locked for security reason!

10 hours ago at 3:20 PM

From iSupport ID >

Hide

To [redacted]

Dear User,

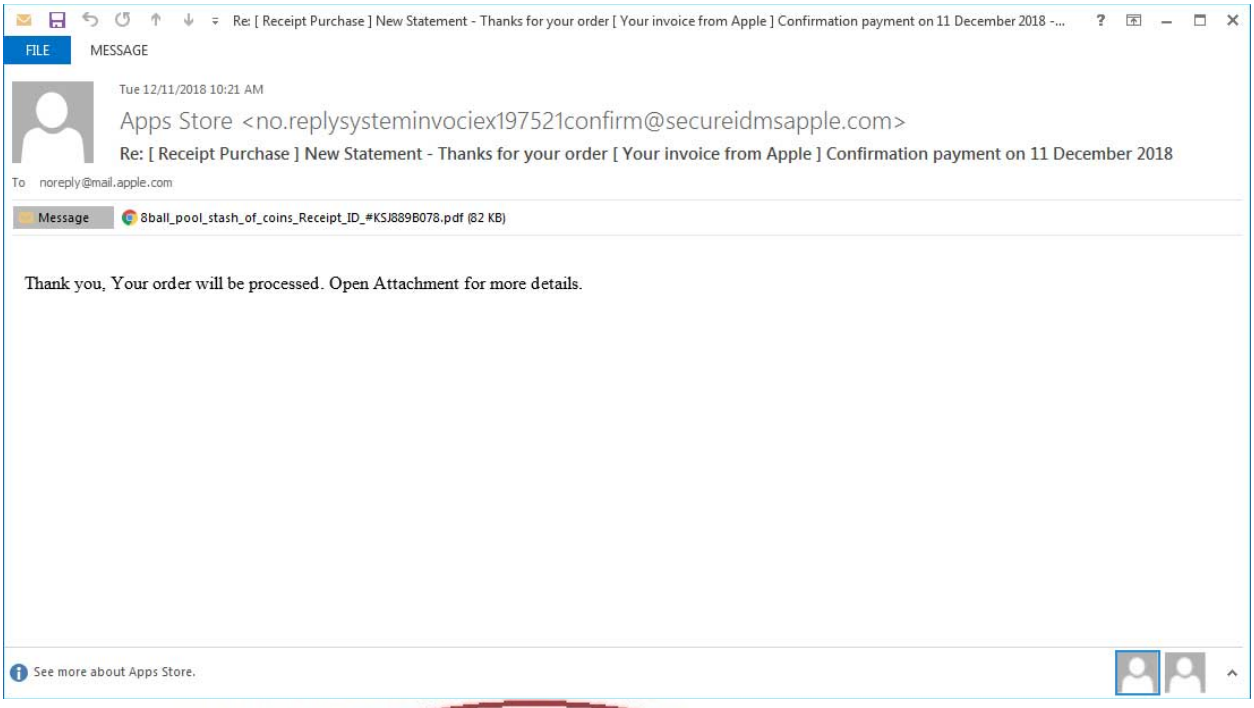
[redacted] was used to sign in to a new web browser.

[redacted] has been temporarily disabled for security reason. When you see this alerts, you can go to HERE to unlock your account.

Your Account will permanently disabled if you do not verify your account under 24 hours

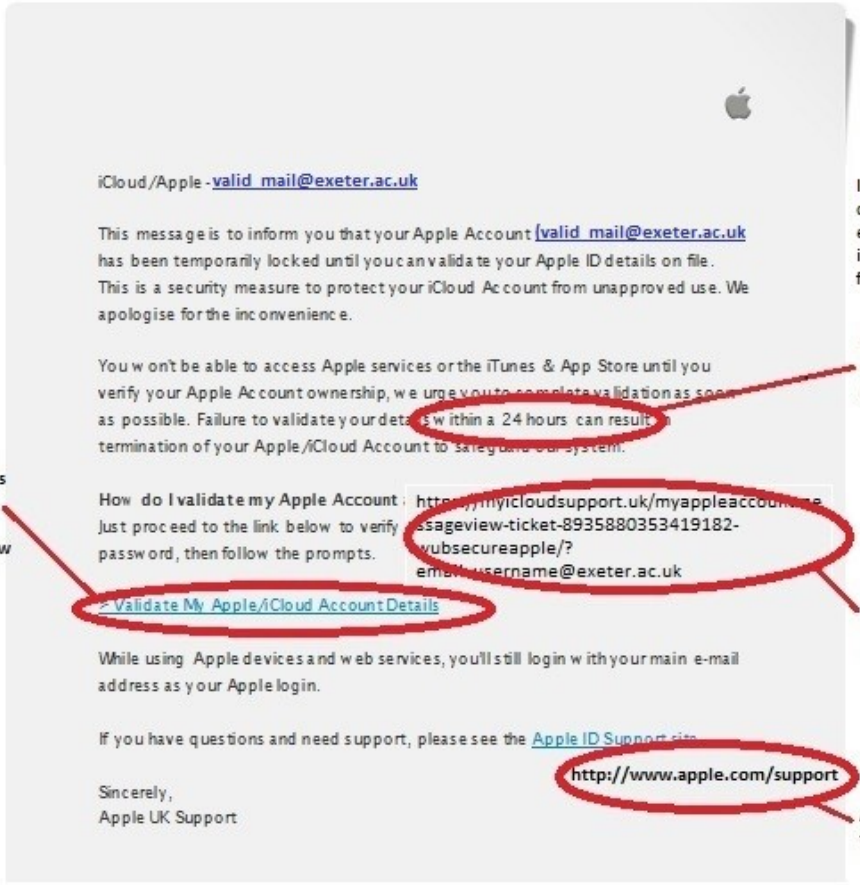
Apple Information

Apple ID | Privacy Policy



From: Apple <secure@icloudsecurityteam.co.uk>
Subject: Apple ID Temporarily Locked
Date: 22 July 2014 18:44:46 BST
To: <valid_email@exeter.ac.uk>
Reply-To: <secure@icloudsecurityteam.co.uk>

Not an apple email address, but quite believable.



If your apple ID is different from your email address, which it can be, it is missing from this email.

Urgent action required or we'll delete your account

A link to sign into your account. Always use your bookmarks to log into your account, never follow a link in an email.

Hovering over the link shows it is to a rogue web address

All the other links go to valid apple urls

RE: [Summary Report] Statement login and update account 08/05/2017

A

AppleID <187arelt.newcostumerID@intl.iCloud.comupdateyourinfonowforextendyouraccountmailpleasecc

Reply

Fri 04/08, 23:05
You

This message was identified as spam. We'll delete it after 8 days. It's not spam

Apple ID
Account Information Page

We need your help resolving an issue with your account. Thus, we have temporarily lock your account.

We understant it may be frustating not to have full access to your account.

We want to work with you to get your account back to normal as quickly as possible.

How can you help?

It's usually quite straight forward to take care of these things. Most of time, we just need some more information about your account.

Please complete your account informations by clicking in the link below.

Confirm My Account

We will permanently lock your account if we don't receive your verification within 24