## PHISHING-SCAMS: DEFINITION GUIDE

arizona complete health

This guide provides phishing-scams-identity theft common types and definitions.

| Phishing | Scams |
|---|---|
| The fraudulent practice of sending emails or other messages intending to be from reputable companies-organizations to persuade a person to reveal personal-protected-identifiable information, such as passwords and credit card numbers. | A dishonest scheme, or fraudulent activity. Someone who makes monetary gain using illegal techniques, trickery to get personal-protected-identifiable information, such as financial, housing, and personal information. |
| **Identity Theft** | **Fraudulent Activity** |
| The fraudulent acquisition and use of a person's (victims) confidential-private identifying information, usually for financial gain. Is when someone uses personal information to open new accounts or make transactions in a person's (victims) name. | Is deliberate deceitful, dishonest, or untrue activity. Is about wrongful-criminal deception intended to result in financial or personal gain. |
| **PHI: Protected Health Information** | **PII: Personally Identifiable Information** |
| Is any information in the medical record or designated record set (date of birth, medical certificates, license information, vehicle registration details) that can be used to identify an individual and that was created, used, or disclosed while providing a health care service such as diagnosis or treatment. | Is any type of data that can be used to identify someone, from their name and address to their phone number, passport information, and Social Security numbers. This information is frequently a target for identity thieves, especially over the internet. |
| **Common Scam Definitions** | |
| Advance fee | An advance-fee scam is a form of fraud and is one of the most common types of confidence tricks. The scam typically involves promising the victim a significant share of a large sum of money, in return for a small up-front payment, to the fraudster. |
| Amazon gift card | A person is prompted to pay using Amazon.com or other Gift Cards sold on Amazon and to provide the claim codes via email or phone, this can be a scam. A legitimate transaction using Amazon Gift Cards can only be completed through the Amazon checkout page and will never occur off Amazon.com. |
| Amazon Prime Video | On the phone, the scammers will ask them to share the two-factor authentication code sent to their device by Amazon. Doing so will give the scammer access to their Amazon account. |
| Amazon "write a review" | Fraudsters send emails that offer money in return for writing product reviews on Amazon. |
| Brushing | In e-commerce, brushing, also called "review brushing", is a deceitful technique sometimes used in e-commerce to boost a seller's ratings by creating fake orders, which are either shipped to an accomplice or to an unsuspecting member of the public. |


Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
TransUnion. https://www.transunion.com/identity-protection
The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
Amazon. https://www.amazon.com/gp/help/customer/display.html?nodeId=G4YFYCCNUSENA23B
theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

## PHISHING-SCAMS: DEFINITION GUIDE

arizona complete health

| | |
|---|---|
| Business opportunity-employment | Employment or job scams are usually a form of advance fee fraud where unscrupulous persons posing as recruiters or employers offer attractive employment opportunities that require the job seeker to pay money in advance. |
| Cashier's check | A person receives payment via a cashier's check and is supposed to deposit the payments to an account and forward the money to somebody else. Often advertised as a work-at-home check processing job, these schemes are often problematic. In some cases, this is about laundering money for criminals. |
| Emergency | Emergency scams usually target parents, grandparents, or other family members. Someone calls or sends a message claiming to be a child or grandchild in trouble or the friend of a family member who is in trouble and urges the victim to wire money immediately to help with an emergency. |
| Fake giveaway | Person gets a call, email, or letter saying they won a sweepstakes, lottery, or prize — like an iPad, a new car, or something else. But the person can tell it's a scam because of what they do next: Fraudster asks the person to pay money or give them their account information to get the prize. |
| Fake invoice | Is a type of fraud in which fraudsters send fake invoices to a business. Fraudsters sometimes also notify the business that a vendor's details have changed and provide wrong information to defraud the company. |
| Fake job | Employment or job scams are usually a form of advance fee fraud where unscrupulous persons posing as recruiters or employers offer attractive employment opportunities that require the job seeker to pay money in advance. |
| Fake listing | A person portrays themselves to be a Real Estate agent and collects payment from an apartment seeker, without owning the listing or premise. The transaction can occur in person, by phone or email with original contact being made through online posting on third party websites, such as Craigslist. |
| Fake refund | Is about getting refunds without returning goods. For example, a customer buys an item, requests a refund once they get it, then makes a false claim that prevents them from sending the item back to you. |
| Foreign Exchange Money | Foreign exchange fraud is any trading scheme used to defraud traders by convincing them that they can expect to gain a high profit by trading in the foreign exchange market. |
| Home Repair | They pressure a person to act quickly and might ask them to pay in cash or offer to get them financing. But |


Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
TransUnion. https://www.transunion.com/identity-protection
The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
Amazon. https://www.amazon.com/gp/help/customer/display.html?nodeId=G4YFYCCNUSENA23B
theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

## PHISHING-SCAMS: DEFINITION GUIDE

| | |
|---|---|
| | here's what happens next: the fraudsters run off with the person's money and never make the repairs. Or they do shoddy repairs that make things worse. Maybe they got the person to sign a bad financing agreement that puts your house at risk. |
| IRS Imposter | Imposter scammers pretend to be from the IRS or Social Security, a business, or a charity. They want the person to trust them so they can steal personal information and money. |
| Mystery box | Revolves around an exciting promise: the person can win a box filled with high-value gadgets and smart devices just by completing a survey and paying a small delivery fee. It sounds too good to be true, right? Unfortunately, that's because it is. |
| Off-Platform Payment | Off-Platform Instance means an instance of Digital Retailing on any Customer Application. All official Amazon purchases are done on the platform. However, some fraudulent sellers on Amazon will try to get users to pay them off the platform and use payment methods such as Zelle, Venmo or a wire transfer. |
| Overpayment | An overpayment scam, also known as a refund scam, is a type of confidence trick designed to prey upon victims' good faith. In the most basic form, an overpayment scam consists of a scammer claiming, falsely, to have sent a victim an excess amount of money. |
| Phishing | Phishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source |
| Porch pirate | Refers to people who steal packages that are left on porches, stoops, and steps. |
| Shopping Spree | Person gets a phone call, offering them a "$500 shopping spree" (or another amount). Fraudsters say they're from a well-known company or a government agency. Then, the caller asks for bank account number to collect a small fee. Fraudsters say the fee is for shipping and handling of vouchers. It's a scam! |
| Spoofing | Spoofing is when someone disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince a person that they are interacting with a trusted source. |
| Tech Support | A technical support scam, or tech support scam, is a type of scam in which a scammer claims to offer a legitimate technical support service. Victims contact scammers in a variety of ways, often through fake pop-ups resembling error messages or via fake "help |


Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
TransUnion. https://www.transunion.com/identity-protection
The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
Amazon. https://www.amazon.com/gp/help/customer/display.html?nodeId=G4YFYCCNUSENA23B
theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

| | |
|---|---|
| | lines" advertised on websites owned by the scammers. |
| Typo squatting | Also known as URL hijacking, is a form of cybersquatting (sitting on sites under someone else's brand or copyright) that targets Internet users who incorrectly type a website address into their web browser (e.g., “Goooogle.com” instead of “Google.com”). |
| Unclaimed package | A package delivery scam happens when a person gets an unsolicited text message about an unclaimed delivery, with a malicious link to supposedly “claim” the package that doesn't exist. |
| **Common Phishing Definitions** | |
| Angular | Is a new type of phishing attack that targets social media users. People disguise themselves as a customer service agent on social media to reach a disgruntled customer and obtain their personal information or account credentials. |
| Clone | Is a form of email-based threat with a particularly nasty twist. Attackers clone a genuine email with attachments or links so that it looks like it comes from a known sender or a company a person does business with. |
| Deceptive | Use deceptive technology to pretend they are with a real company to inform the targets they are already experiencing a cyberattack. The users then click on a malicious link, infecting their computer. |
| Domain | Is a scam to trick email recipients into handing over their account details via links in emails posing as their registrar. The links forward unsuspecting domain owners to dodgy replica registrar websites looking to obtain sensitive information such a domain account's username and password. |
| Email | The general term given to any malicious email message meant to trick users into divulging private information. Attackers generally aim to steal account credentials, personally identifiable information (PII) and corporate trade secrets. |
| Evil-twin | is a cyberattack in which a hacker creates a fake Wi-Fi access point that mimics a legitimate network and tricks users into connecting. Threat actors create such hotspots to infiltrate a device and gain unauthorized access to sensitive data. |
| HTTP | A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. |

Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
TransUnion. https://www.transunion.com/identity-protection
The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
Amazon. https://www.amazon.com/gp/help/customer/display.html?nodeId=G4YFYCCNUSENA23B
theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

## PHISHING-SCAMS: DEFINITION GUIDE

arizona complete health

| | |
|---|---|
| Image | Uses images with malicious files in them meant to help a hacker steal account info or infect the computer. |
| Man-in-the-middle | Is a type of cyber-attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation. |
| Pharming | Is a sophisticated type of fraudulent activity that redirects internet users to fake websites to steal personal or financial information, such as login credentials, credit card details, or social security numbers. |
| Pop-up | Often uses a pop-up about a problem with the person's computer's security or some other issue to trick them into clicking. The person is then directed to download a file, which ends up being malware, or to call what is supposed to be a support center. |
| Search engine | also known as SEO poisoning, is when cybercriminals use search engine optimization to appear as the top results on a search engine to lead searchers to a spoofed website. SEO poisoning = Search Engine Optimization (SEO) poisoning is a cyberattack technique that manipulates search engine results pages (SERPs) to promote harmful websites. Cybercriminals create or modify web content and employ aggressive search strategies that artificially boost the ranking of malicious web pages for popular keywords. |
| Smishing | Is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information, or sending money to cybercriminals. The term "smishing" is a combination of "SMS"—or "short message service," the technology behind text messages—and "phishing." |
| Social engineering | There are different types of social engineering attacks: Phishing: The site tricks users into revealing their personal information (for example, passwords, phone numbers, or social security numbers). |
| Spear | Spear phishing is a type of phishing attack that targets a specific individual, group, or organization. These personalized scams trick victims into divulging sensitive data, downloading malware or sending money to an attacker. |
| TOAD attack<br>(Telephone-Oriented Attack Delivery) | A TOAD attack is a relatively new form of phishing attack that combines voice and email phishing techniques. Attackers aim to trick users into disclosing |


Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
TransUnion. https://www.transunion.com/identity-protection
The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
Amazon. https://www.amazon.com/gp/help/customer/display.html?nodeId=G4YFYCCNUSENA23B
theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

| | |
|---|---|
| | sensitive information over the phone, such as login credentials or financial data, by impersonating a trusted authority figure. They will get on a call with the victim, claiming to be a representative from a reputable company or organization. Then, they will follow up with an email that contains a phishing link or attachment. |
| Vishing | The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies to induce individuals to reveal personal information, such as bank details and credit card numbers. |
| Watering hole | Works by identifying a website that's frequented by users within a targeted organization, or even an entire sector, such as defense, government, or healthcare. That website is then compromised to enable the distribution of malware. |
| Website | A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. |
| Whaling | Is a spear phishing attack that is aimed exclusively at a high-level executive or official. The attacker typically impersonates a peer within the target's organization, or an equal or higher-level colleague or associate from another organization. |

Experian. https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-identity-theft/
Equifax. https://www.equifax.com/personal/identity-theft-protection/#:~:text=To%20help%20better%20protect%20yourself%20from%20identity%20theft%2C%20use%20Lock,Experian%2C%20and%20TransUnion%20credit%20reports
TransUnion. https://www.transunion.com/identity-protection
The U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html
Amazon. https://www.amazon.com/gp/help/customer/display.html?nodeId=G4YFYCCNUSENA23B
theft/#:~:text=Never%20give%20out%20your%20personal,financial%20accounts%20for%20suspicious%20transactions
Federal Trade Commission. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data