Resource Computer Solutions
Powerfully Proactive IT Business Experts

Phishing Scams & Spam

Phishing emails have always been and always will be a common threat that plagues users across the digital world. With these scams becoming increasingly harder to spot as hackers continuously grow smarter, RCS has compiled a quick guide filled with tips to help you become a phishing identifying expert! Whenever in doubt of the legitimacy of an email use this guide to help you decide if it's safe or not!

Be Skeptical

Don't believe everything you at first glance in your inbox! Many hackers mislead users by making the Headers, Display Names, and Subject Lines mimic well known companies or by writing enticing offers to lure people in. If the offer sounds too good to be true or teh Display Name doesn't match the domain name in the From proceed with great caution! It is most likely a trap.

Look Don't Click

If when you receive an email it's important to remeber that you can preview an email without having to fully open the message. This is a great tool to practice as it can allow you to potentially spot a dangerous email without having to possibly put your device at risk.

Signature & Greeting

Be sure to observe and pay attention to how the email greets you! Most companies and businesses prefer to have their emails be personalized to make them more engaging for customers so they will address you by name. It is not as common anymore for especially large companies to refer to you as simply "Valued Customer." It is also important to look over the SIgnature in the email and make sure that it has company contact information other then just the senders name. Businesses take great care to include contact details such as addresses, contact emails, phone numbers, departments, and at times logo imagery.

Resource Computer Solutions
Powerfully Proactive IT Business Experts

Phishing Scams & Spam

Spell Check

Businesses large and small take great pride and care into making sure all of their material both online and in print have excellent spelling and grammar. If your email has obvious and blatant misspellings with poor grammar it is safe to assume that this email is spam.

You've Won!

Won a prize but not sure how or why? Don't click! Emails that appear and offer you wonderful prizes are often phishing scams trying to win you over with empty promises of fortune and incredible prizes.

Aggressive Language

Fear is a powerful tactic and tool hackers use in order to scare users into doing what they want. Watch out for aggressive language such as "You're account has been suspended," "Immediate action is required," and "Unauthorized login attempt has been made." Stay calm when you read messages like this and don't take any action before assessing the situation fully. The email should not be asking for sensitive and private information in order for you to avoid a major penalty. If you are unsure if the email is authentic then you can contact your bank or whichever company this email claims to be from and inquire about your account through a legitimate source.

Opening Attachments

Careful! Unless you know the sender and were expecting to receive an attachment then you should never randomly open them. Hackers often hide malicious viruses and other harmful material inside attachments, hoping users will open them.

Resource Computer Solutions
Powerfully Proactive IT Business Experts

Phishing Scams & Spam

Covering Expenses

When a message is requesting you to send them payment of some kind in order to cover expenses for something you are to receive this is often a red flag! Proceed with caution and quickly delete the message. Even if the sender did not ask for money in the initial email, you should never send payments for fees and expenses unless you personally know the sender and know the source is legitimate.

Private Information

Never under any circumstances should you send private or sensitive information over email. It is best practice to never send credit card information, account numbers, or passwords over email to anyone as emails are not always a secure line of communication. Legitimate companies and businesses will never ask this of you and should the sender start asking for it then this is a sure sign this is a scam.

Remember!

Phishing emails can pose a serious threat and comes in many disguises. If you ever have any other questions or have accidentally fallen victim to a hacker, don't hesitate to give RCS a call for a free consultation! We specialize in not only disaster recovery and business continuity, but also with solving any issue a hacker may have caused on your devices. With out partners, Resource Computer Solutions will provide the most customized services to each and every customer and their unique needs since not all malicious cyber attacks are the same.

Resource Computer Solutions
1945 West 9th Street, Upland, CA 91786
909 • 949 • 9159
https://resourcecomputer.com