

# WHAT EVERY **SMALL BUSINESS** SHOULD KNOW ABOUT PHISH

### **SMALL BUSINESSES ARE UNDER**

**THREAT** FROM A VARIETY OF SOURCES, BOTH INTERNAL AND EXTERNAL. BUT PHISHING IS THE MOST PRESSING.

#### **STANDARD PHISHING**

Standard phishing is the most common type of phishing. These attacks typically involve mass emails sent to large groups of people.

#### **SPEAR PHISHING**

A targeted attack aimed at a specific individual or organization, often involving the use of personal information to make the email seem more credible.

#### **WHALE PHISHING**

Targets high-ranking executives or other individuals who have access to sensitive information. This kind of attack is more sophisticated as the victims are often techsavvy.

#### VISHING

This attack uses phone calls or VoIP (Voice over IP) messages to trick victims into revealing sensitive information.

Fake Email Address

**Too Generic** 

Urgency

Fake Link

Grammar Error

# New Message to: me

#### subjetc: Amazon Account Suspended

from <amazeon-security@hotmail.com>

Amazon Account Suspended Amazon <amazeon-security@hotmail.com> Inbox July 12, 2021 at 10:09 AM

#### Your Account Is Temporarily Suspended! Hello user We temporarily suspended your Amazon account due to multiple unauthorized accesses

detected by our services. To reinstate your account, we recommend that you update the information within the next 24\* hours. Otherwise, your account will be permanently suspended.

#### Update Your Information << http://info@amazonhelp.art>> We hope to see yuo again soon.

Best, **Amazon Security Team** 



## PHISHING PREVENTION BEST PRACTICES

#### WATCH FOR OVERLY GENERIC CONTENT

Cybercriminals send a large batch of emails. Look for examples like "Dear valued customer."

#### LOOK FOR ERRORS

Notice misspellings, incorrect grammar and odd phrasing. This might be a deliberate attempt to try to bypass spam filters.

#### **EXAMINE THE "FROM:" EMAIL ADDRESS**

The first part of the email address may look legitimate, but the last part might be off by a letter or may include a number in the usual domain.

#### LOOK FOR URGENCY

"You've won! Click here to redeem prize," or "We have your browser history pay now or we are telling your boss."

#### **CHECK ALL LINKS**

Hover over the link and see whether the link's description matches with the one implied in the email.

#### **CHECK FOR SECURE WEBSITES**

Any webpage where you enter personal information should have a url with https://. The "s" stands for secure.

#### **DON'T CLICK ON ATTACHMENTS**

Attachments containing viruses might have an intriguing message encouraging you to open them such as "Here is the schedule I promised."

### **3 STEPS TO PROTECT YOUR BUSINESS**

#### **CONDUCT** REGULAR SECURITY AWARENESS TRAINING

Keep your employees prepared to deal with any security threats that come your way by keeping them up to date on the latest security landscape and best practices through regular training.

#### **PERFORM** ROUTINE TESTING, TO SEE WHETHER THE **TRAINING IS EFFECTIVE**

It's critical to consistently evaluate the success of your security training through quizzes, surveys and mock tests.

#### **DEPLOY** QUARANTINING SOLUTIONS THAT STOP PHISHING ATTACKS

Businesses can protect themselves from the harmful effects of phishing attacks by deploying quarantining solutions that help stop phishing attempts in their tracks.



**CONTACT US** (757) 321-9433



