SEPTEMBER 10, 2021 // FRIDAY // ISSUE 1

SECURITY NEWS

PHISHING ATTACKS HAVE INCREASED BY 22% THIS YEAR

New Information Technology employee Chris McDaniel.

New IT Staff Member

CHRIS MCDANIEL
SEPTEMBER 2021

The Yadkin County Information Technology Department would like to introduce the newest member of our team, Chris McDaniel. Chris will be our new Cybersecurity Specialist for the county and will help bring the county's security posture to a whole new level. Chris holds a Master's Degree in Cybersecurity from ECPI University and has been working in the IT field for almost 10 years now. He has a wife and 3 children, 2 girls, Addison (9) and Ainsley (4), and 1 boy, Maverick (1). Chris is very excited to become a member of the IT Department and the County of Yadkin. He is looking forward to making Yadkin County a secure place not only for the employees but for the citizens as well. Let's give him a big welcome aboard and we wish him well as a member of Yadkin County.

Phishing Attacks

NC DIT
SEPTEMBER 2021

The volume of phishing attacks has increased 22% this year compared to the first half of 2020, according to researchers at PhishLabs, a cybersecurity threat intelligence company that offers anti-phishing, anti-malware, and other ecrime management services. Researchers say, "Phishing continues to be one of the top threats to enterprises with attack volumes outpacing the first half of 2020 by 22%." They report that phishing is the primary way that cyber attackers use to steal credentials, hijack accounts, and compromise organizations.

While phishing continues to thrive, social media is increasingly being used for impersonation, fraud, and other cyber threats. Threats targeting enterprises via social media grew 47% in the first half of 2021, showing that to be a top threat vector. The researchers found that fraud-related attacks were the most common form of phishing on social media, while payment services and the healthcare industry were highly targeted by these attacks.

The report from PhishLabs may be found via the link: PhishLabs Report

"Payment services and healthcare experienced the steepest increases in social media attacks per business in Q2," the researchers write. "Payment services, which ranked the highest of all industries, increased threat activity by over 500% when compared to Q1. Healthcare experienced the second highest increase in activity from Q1 to Q2, moving up in rank from 17th to 10th, due to a 188% increase in attacks per business in Q2."

PhishLabs also found that attacks targeting single sign-on (SSO) solutions rose by 40% in Q2 compared to Q1. The greatest risk to corporate email users, however, are credential theft phishing and response based attacks, such as Business Email Compromise (BEC). According to PhishLabs, BEC-type attacks accounted for 96% of threats found in enterprise inboxes. Researchers say, "These threats continue to evade email security controls at a high rate."

One of the best ways to reduce the risk of these phishing attacks is to provide security awareness training with realistic phishing emails that mimic real threats. By providing individuals the opportunity to see and respond to these types of attacks in a safe environment, it reduces the risk when a real threat occurs.

SEPTEMBER 10, 2021 // FRIDAY // ISSUE 1

SECURITY NEWS

SCAM ALERTS

Hurricane-Related Scams

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
SEPTEMBER 2021

The 2021 Atlantic hurricane season began on June 1, 2021 and will end on November 30, 2021. This is when cyber attackers take advantage of this dangerous time of year and promote malicious hurricane themed attacks.

The Cybersecurity and Infrastructure Security Agency (CISA) warns users to remain on alert for malicious cyber activity targeting potential disaster victims and charitable donors following a hurricane. Fraudulent emails, often containing malicious links or attachments, are common after major natural disasters. Exercise caution in handling emails with hurricane-related subject lines, attachments, or hyperlinks. In addition, be wary of social media pleas, texts, or door-to-door solicitations relating to severe weather events.

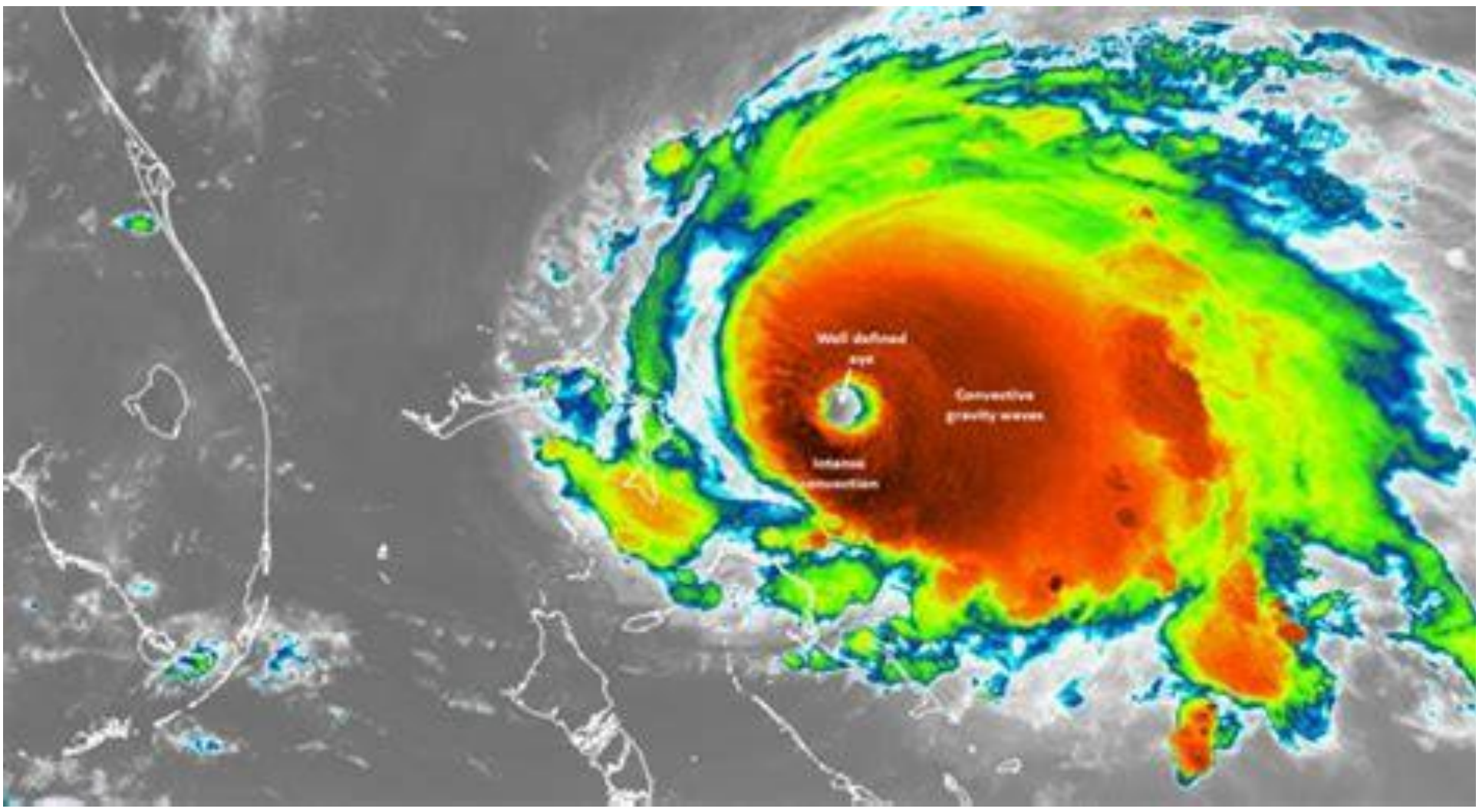
To avoid becoming victims of malicious activity, users and administrators should review the following resources and take preventative measures.

- Staying Alert to Disaster-related Scams
- Before Giving to a Charity
- Staying Safe on Social Networking Sites
- Avoiding Social Engineering and Phishing Attacks
- Using Caution with Email Attachments

If you believe you have been a victim of cybercrime, file a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) at www.ic3.gov.

Cybersecurity and Infrastructure Security Agency (CISA)

The information for this article came from the North Carolina Department of Information Technology and can be found at link provided: NCDIT



ATTACKS AND SCAMS

Vishing – Phone Call Attacks and Scams

Jen Fox, SANS, May 3, 2021

Example of How to Defend Yourself Against Vishing Attacks

Overview

When you think of a cybercriminal you probably think of an evil mastermind sitting behind a computer, launching sophisticated attacks over the internet. While some of today's cyber criminals do use advanced technologies, many simply use the phone to trick their victims. There are two big advantages to using a phone: Unlike other attacks, there are fewer security technologies that can detect and stop a phone call attack; also, it is much easier for criminals to convey emotion and build trust over the phone, which makes it easier to trick their victims. Let's learn how to spot and stop these attacks.

How Do Phone Call Attacks Work?

First, understand that these criminals are usually after your money, information, or access to your computer (or all three). They do this by tricking you into doing something you should not do, a technique called "social engineering." Cyber criminals often create situations that feel very urgent and realistic on the call. Some of the most common examples include:

- The caller pretends they are from the government and informs you that you have unpaid taxes. They explain that if you don't pay your taxes right away you will go to jail, then pressure you to pay your taxes with your credit card over the phone. This is a scam. The government will send official tax notifications only by regular mail.

- The caller pretends to be from a company such as Amazon, Apple, or Microsoft Tech Support and explains that your computer is infected. Once they convince you that your computer is infected, they pressure you into buying their software or giving them remote access to your computer.

- An automated voicemail informs you that your bank account or credit card has been canceled, and you have to call a number back to reactivate it. When you call, you get an automated system that asks you to confirm your identity as well as all sorts of private questions. This is really not your bank. They are simply recording all your information for identity fraud.

Protecting Yourself

The greatest defense you have against a phone call attack is yourself. Keep these things in mind:

- Anytime anyone calls you and creates a tremendous sense of urgency or pressure, be extremely suspicious. They are attempting to rush you into making a mistake. Even if the phone call seems OK at first, if it starts to feel strange, you can stop and say "no" at any time.

- Be especially wary of callers who insist that you purchase gift cards or prepaid debit cards.

- Never trust Caller ID. Bad guys will often spoof the number, so it looks like it is coming from a legitimate organization or has the same area code as your phone number.

- Never allow a caller to take temporary control of your computer or trick you into downloading software. This is how they can infect your computer.

- Unless you placed the call, never give the other party information that they should already have. For example, if the bank called you, they shouldn't be asking for your account number.

- If you believe a phone call is an attack, simply hang up. If you want to confirm that the phone call was legitimate, go to the organization's website (such as your bank) and call the customer support phone number directly yourself. That way, you really know you are talking to the real organization.

- If a phone call is coming from someone you do not personally know, let the call go directly to voicemail. This way you can review unknown calls on your own time. Even better, on many phones you can enable this by default with the "Do Not Disturb" feature.

Scams and attacks over the phone are on the rise. You are the best defense at detecting and stopping them.

Report the Crime

A real technician who steps in to salvage a computer after a malware incident would strongly advise consumers to change passwords on accounts, notify their banks and credit card companies, and monitor financial transactions closely. Consumers in the U.S. should also report vishing calls to The Federal Trade Commission online. The FBI's Internet Crime Complaint Center also handles vishing investigations.

Although vishing and its online cousin phishing aren't going away anytime soon, vigilance and a strong dose of skepticism can help reduce the risk of loss from these types of scams.

The information in this article was provided by SANS