The Monthly Security Awareness Newsletter for You

# Personalized Scams

## Overview

Cyber criminals continue to come up with new and creative ways to fool people. A new type of scam is gaining popularity—personalized scams. Cyber criminals find or purchase information about millions of people, then use that information to personalize their attacks. Below we show you how these scams work and walk you through a common example. The more you know about these scams, the easier it is for you to spot and stop them.

## How Does it Work?

Email or phone call scams are not new, cyber criminals have been attempting to fool people for years. Examples include the "You Won the Lottery" or the infamous Nigerian Prince scams. However, in these traditional scams cyber criminals do not know whom they are targeting. They simply create a generic message and send it out to millions of people. Because these scams are so generic, they are usually easy to spot. A personalized scam is different; the cyber criminals do research first and create a customized message for each intended victim. They do this by finding or purchasing a database of people's names, passwords, phone numbers, or other details. This type of information is easily available due to all the websites that have been hacked. It is also commonly available on social media sites and in publicly available government records. The criminals then target everyone they have information on.

One common trick cyber criminals use is fear or extortion to force you into paying them money. The attack works like this. They find or purchase information on people's logins and passwords obtained from hacked websites. They find your account information included in such a database and send you (and everyone else in the database) an email with some personal details about you, including the original password you used on the hacked website. The criminal refers to your password as "proof" of having hacked your own computer or device, which is of course not true. The criminal then claims that while they hacked your computer they also caught you viewing pornography online. The email then threatens that if you do not pay their extortion fee, they will share with your family and friends evidence of embarrassing online activities.

The catch is, in almost every situation like this the cyber criminal never hacked your system. They don't even know who you are or which websites you've visited. The scammer is simply attempting to use the few personal details they have about you to scare you into believing they hacked your computer or device, and to trick you into paying them money. Remember, bad guys can use the same techniques for a phone call scam also.

## What Should I Do?

Recognize that emails or phone calls like these are a scam. It's natural to feel scared when someone has personal information about you. However, remember the sender is lying. The attack is a part of an automated mass-scale campaign, not an attempt to directly target you. It is becoming much easier for cyber criminals today to find or purchase personal information, so expect more personalized scams like these in the future. Some clues to look for:

- **Whenever you receive a highly urgent email, message, or phone call be very suspicious. If someone is using emotions like fear or urgency, they are trying to rush you into making a mistake.**
- **When someone is demanding payment in Bitcoin, gift cards, or other untraceable methods.**
- **When you get a suspicious email, search on Google to see if other people have reported similar attacks.**

Ultimately, common sense is your best defense. However, we also recommend you always use a unique, long password for each of your online accounts. Can't remember all your passwords? Use a password manager. In addition, enable two-step verification whenever possible.

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

## Guest Editor

***Lenny Zeltser*** *is a cybersecurity veteran. He builds anti-malware solutions at Minerva Labs and teaches security classes at SANS Institute. His experience also includes managed security services and consulting. Follow him at zeltser.com/blog and on Twitter @lennyzeltser.*

## Resources

| | |
|---|---|
| Social Engineering: | https://www.sans.org/u/MUU |
| Stop That Phish: | https://www.sans.org/u/MUZ |
| Search Yourself Online: | https://www.sans.org/u/MV4 |
| Password Manager: | https://www.sans.org/u/MV9 |