CYBER SECURITY Newsletter

USING EMAIL SAFELY

The Problem

Email has become one of the primary methods to communicate, both at work and at home. Email is an extremely powerful tool allowing you to reach anyone around the world instantly. Email is simple; you type your message, include attachments, and send. Email is also cheap and sometimes even free. Given all of the above, it is not unusual for individuals to send or receive hundreds of emails a day.

The danger is cyber criminals leverage this technology as well. It is very simple for a cyber criminal to create emails pretending to be someone or something you trust, such as your bank or your favorite online store. In addition, cyber criminals send out literally millions of these malicious emails every day. Email has become a cheap and effective way to attack people around the world. As a result, you need to use email carefully. In this newsletter, we discuss the most common email attacks and the steps you can take to protect yourself, your family, and our organization.

Protecting Yourself

The number one step to protect yourself is to **be suspicious,** because most email sent today is spam, scams, or malicious attacks. While security programs block most of these attacks, some will always get through. If you receive an email that looks odd or sounds too good to be true, it probably is.

Links and Attachments: One of the simplest ways for a cyber criminal to infect your computer is for you to accept a malicious attachment or link pointing to a malicious website they have created. To protect yourself, only click on links or open attachments if you are expecting them. If you are not sure the email is legitimate, contact your IT help desk or security team.

Privacy: Be careful of what you send in an email. When you send an email across the internet, that email can be intercepted and read, just like a postcard. In addition, email is permanently archived and stored forever. If you have something highly confidential to communicate, encrypt the email or call the person instead.

Using Email Safely

Email has become one of the fastest and simplest ways to communicate around the world. As a result, it has also become one of the primary methods cyber criminals will use to attack you on the Internet.

Idaho State UNIVERSITY

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

Spear Phishing

So far, all the attacks we have discussed are designed to attack as many people as possible. However, cyber criminals have developed an even more dangerous type of attack called Spear Phishing. This type of attack is when criminals target you or our organization. Instead of sending out millions of emails, they only send a few emails specifically targeting certain individuals in our organization.

The reason these targeted attacks are more dangerous is because the criminals do extensive research first. They learn who works in our organization, who you communicate with, and what your internal emails look like. They then create customized emails based on this information and send these emails to specific individuals. As a result, when the intended target receives these emails, they are often fooled and fall victim.

Since there are so few emails being sent, spear phishing attacks are harder to detect. These attacks are often missed by anti-virus or email filters. Remember, if an email or message seems suspicious, it most likely is an attack. If you are not sure, contact your help desk or information security team.

The Attacks

Email is cheap, fast, and simple; it is the perfect way to communicate. As a result, email is also the perfect method to attack millions of people around the world. Here are three of the most common email attacks to be aware of:

Malicious Attachments and Links: Cyber criminals send emails that look like they come from legitimate organizations, such as your bank, from a trusted friend, or perhaps even a co-worker. They do this by forging the "From Address" or by including real logos. The goal of the email is to trick you into opening an attachment. The criminals create convincing stories, such as informing you that your computer is infected and you must install the attachment to fix it. Or they say you must read the attachment because it includes important information for you. If you open the attachment, your computer will be infected and, if successful, the cyber criminal will have total control of your system. Additionally, cyber criminals can include links in emails taking you to malicious websites. These websites then attack and attempt to infect your computer.

Even though you have anti-virus software installed, that does not mean you are protected, because cyber criminals have developed new viruses that are undetectable by anti-virus software. If you receive an email you were not expecting, do not open any attachments or click on any links.

Phishing: The goal of phishing is not to infect your computer, but to steal your information. Criminals do this by sending emails pretending to be someone you trust, such as your bank. The emails will inform you that your bank account needs to be updated. They will include a login link to your bank for you to update your information.

However, the email is a scam. If you click on the link, it directs you to a website resembling your bank, but in reality it was developed and is controlled by the cyber criminal. If you enter your information, you are providing your online banking information to cyber criminals who will use it to steal your money. Never visit your bank or any other important website by clicking on links in an email. Instead, always type the URL in your browser so you know you are going to the correct website.

Scams: These emails use the same attack methods that criminals have been using for thousands of years. Cyber criminals fool you so they can steal your money or hoax you into providing your information with a lie conveyed through email. For example, they will say you have won the lottery and ask you to call a phone number to collect your prize. If you call, they will inform you that you must pay taxes on the prize. Once you pay the money, the cyber criminal will disappear, and will most often never be found. Remember, if a deal sounds too good to be true, it most likely is.