CYBER SECURITY newsletter

USING EMAIL SAFELY

The Problem

Email has become one of the primary methods people communicate, both at work and at home. Email is extremely powerful, you can instantly reach anyone around the world. Email is simple; you just type what you want to say, include attachments, and hit send. Email is cheap, sometimes even free. Given all these factors it is not unusual for individuals to send or receive hundreds of emails a day.

The danger is cyber criminals can leverage this technology as well. It is very simple for a cyber criminal to create emails that pretend 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 to look out for and steps you can take to protect yourself, your family, and our organization.

Protecting Yourself

Be Suspicious: The number one step to protecting yourself is to be suspicious. Over 90% of email sent on the Internet 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 to ask you to infect it for them. They do this by sending emails with malicious attachments or links pointing to malicious websites. To protect yourself, only click on links or open attachments if you are expecting them. If you are not sure if 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 use to attack others on the Internet.

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

Spear Phishing

So far all of 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 bad guys are targeting specifically you or our organization. Instead of sending out millions of emails, they only send out twenty or thirty, all targeting specific individuals or a specific organization.

The reason these targeted attacks are more dangerous is because the criminals do their research. They learn who works in our organization, who we communicate with and what our 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 victim 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. As always, if an email or message seems suspicious, it most likely is an attack. If you are not sure, contact your IT 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 with which to attack millions of people around the world. Here are three of the most common email attacks to look out for.

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

Just because you have anti-virus software installed does not mean you are protected. Cyber criminals have developed new viruses that cannot be detected by anti-virus software. If you receive an email you did not expect, 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 something you trust, such as your bank. The emails will tell you that your bank account needs to be updated and then include a link to login to your bank and update your information.

However, the email is a lie. If you click on the link it takes you to a website that looks like your bank, but in reality is controlled by cyber criminals. If you enter your information, thinking you are logging into your bank, you are really giving your online banking information to cyber criminals who will then 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. That way you know you are going to the correct website.

Scams: These emails use the same attack that criminals have been using for thousands of years. The cyber criminals fool you out of your money or trick you for your information with a lie conveyed through email. For example, they will tell you that you have just won the lottery and ask you to call a phone number to collect your prize. If you call them, they will tell you that you have to pay taxes on the prize first. Once you pay the money, the cyber criminal disappears and you will never hear from him again. If a deal sounds too good to be true, it most likely is.