Computer-Ease

Complete Computer Solutions
www.CVWare.com

Custom Programming IT Services Network Management Websites Computers

Good afternoon all! So today we deep dive into email and how to help keep yourself out of trouble!

Email is the primary entry point for most things into our computers and as such it is a pretty large topic. We all hear about phishing and unsolicited email etc… and the truth is that email is the area where most bad things happen or start, and this is where the most critical concern is. And, although we are busy and in a hurry, THIS is where we need to stop and think!

Everyday we see spam and unsolicited emails in our inbox or spam folders, and while these are usually pretty obvious, the emails that are NOT obvious are usually far more insidious. As I have outlined before, there needs to be attention paid to these and understand what not to do. And unfortunately, many emails can come from "someone we know" or from an address that appears to be from someone we know, making it all that much harder.

Understanding not to click on links in an email, (even if you DO know the person sending the email to you), is a critical concept, and understanding that every email could potentially be a problem, and that links are bad in email's is the key thing to understand here.

Additionally, many emails also request you to just 'give them a call' if you have any questions. And while you may not think this is as bad… you would be mistaken. Bad actors work very hard at making things believable, and this includes having the right person be on that phone when you call.

In-fact, right now there are serious threat emails circulating saying it is from an "anti-virus service" (Norton or McAfee usually) which just renewed and is 'informing you' about the amount and a receipt or invoice.

These emails are trying to get you to call and talk to someone, and once you do, they say they can reverse the charge, however they need access to your computer or account. Instead of calling or clicking, if your worried about it, call your credit card company and ask about the charge – chances are it is bogus and you should just delete the email.

A couple of other emails that we see all the time say they are from PayPal and Amazon, and are about 'your order', and again they are trying to get you to either click on the link, or give them a call. These are phishing emails, and are attempting to get you to click on the link to 'your account' and then login. Their goal is to get your user name and password to PayPal or Amazon, and these phishing emails work on many people!

In this time of hackers, scammers and con-men, we must realize that it is critical to treat **ALL** email as suspicious – even when it appears that it is from someone we may very well know and trust. Friends, family, and yes even businesses and clients can be a threat if their system is compromised. The bad guys get your email from website breaches, paid lists of valid emails for marketing purposes, or from hacking an email account or computer. The latter type is preferred since it is a 'known entity' and usually they have some time before the breach is discovered.

It is extremely common for an email to come from a compromised email system to a person they know. Usually, this email has an unusually short sentence, (more like a few words really), and then a link to

something. Typically the email will say something like “thought you might like this” or “what we discussed” and then the link – very short, trying NOT to give away that the person you know didn’t actually send it.

Other common emails usually include larger institutions or websites, (Chase bank, Facebook, Apple, Citi bank, AT&T, Verizon, DHL, FedEx etc...) these emails usually attempt to tell you “something is wrong” with your account and that you need to log in and take care of it. As with the ‘anti-virus scheme’, some discuss and ‘order placed’ and that it needs your final approval, and others contain an ‘invoice’ or ‘receipt’ for a transaction etc. Over 98% of the time, these emails contain a link that may look real, but it takes you to someplace other than you think, and that will get you into trouble quick. (Sometimes it is only a ‘please call’ message and then a phone number.)

And many bad emails contain a PDF, Word document or ZIP file that is ‘showing the invoice’, however these also usually contain a virus, Trojan or other nefarious method to hook you!

And then many times an email will contain a link to an “unsubscribe” button or link, which is NOT going to unsubscribe you. In-fact, clicking on the “unsubscribe link” in a spammer email validates that your email is valid and can contribute to many more spam emails. In a hostile email, clicking that “unsubscribe link” can be devastating! (Now, unsubscribing from a legitimate email can usually help you – and is good, and I will explain the difference shortly.)

Bottom line – you should never… and I will repeat that **NEVER** click on links from your email, unless you are a) expecting an email from that business or person and b) 100% positive that the link is going where you think it should! (And honestly... it is pretty darn easy to fool most people!)

Now… all that can be challenging all by itself, and there is quite a lot here… so here the rule is – just don’t click it! Instead do the following:

If the email is a business – then go to that businesses website <u>with your REGULAR bookmark.</u> (ie NOT using the links in the email!!) And then see what they want. If it is a legit email, then you will find the issue / note on their website.

If the email is from a person you know, ask them what the link is about, and if it is legit and they did want you to ‘check it out’ - still use caution, and TALK to them when you ask – and don’t email them! The email reply you get back could be a hacker that has control of their account.

OK, so we have identified a few things and how to not fall for them, but what about some steps to have your email help you stay safe?

One of the biggest issues with email is the bombardment of email. While receiving legitimate emails from legitimate companies that you have services or accounts with, and many times is required and a good thing, it can also lead to many emails from their marketing that the brain can become numb to them and suddenly one faked email that **looks** real just slips through our brain. Not too mention that ‘off moment’ when your busy, tired, not awake yet, or your just at a weak moment. The bad guys look for this moment, and the continued bombardment of email is meant to find you at your weak spot!

One good method of preventing the brain hit of these emails is to have different email addresses or alias emails for different processes. Having one email for services, a different email for purchasing, a

different email for financial, and a different email for family / friends. This might sound like a lot of work, however it can be a huge help for your brain to compartmentalizing these issues.

As an example, if you use emailxx@yahoo.com for purchasing, and email xx123@gmail for services like financial, then getting an email at emialxx@yahoo.com "from Chase Bank" about "your account" you know instantly that it is a fake.

Many email accounts also have the ability to have alias addresses and these can come in quite handy as well. Having yourname123@gmail.com and creating either temporary or permanent aliases such as yourname123+CitiB@gmail.com, or yourname123+Fidel@gmail.com or yourname123+NetFlx@gmail.com etc, can help you assign aliases and setup for segmented emails which can really help control the incoming email hoard. There are many methods to do this, and various email systems have various methods and these are a great way to make things better.

Email filters are also an excellent method to help dissect and manage email as well. Having a couple of simple filters which can route known email addresses to one folder, and unknown email addresses to an unknown folder, is an amazing way to cut down on the flurry of incoming emails.

And just by having a simple check for incoming emails against your address book, and then direct emails accordingly is a quick, simple method which can be a huge help to manage email as well. Many people don't use this, but it can be a HUGE advantage to understand what emails are really about.

And finally we need to discuss unsubscribing from legitimate companies. This one is a little tougher to manage, but with a REAL legitimate email you have the ability to click on the unsubscribe and start that process. The catch… is determining what is real and what is a spammer!

Example… you get that email from Kohls about the new sale. However, is the email REALLY from Kolhs marketing or a spammer? This question is typically answered by 'who the email is from'. Legitimate companies either use a marketing service or an in-house service. If the email says it comes from a legitimate company, (ie kohls.com, or amazon.com, etc), then chances are the email will be coming from an in-house marketing system. If the email came from a bulk email service, then there is a possibility that it is not legit, however, it should show the proper company that it has come from.

And then, if the email says it is from xyz@gmail.com or SoAndSo@xyz.org, then the email probably is NOT from the real company and is from a spammer.

If we hover our mouse over the unsubscribe link in these emails, you should typically see a link which HAS the companies name in it. (not always, it depends upon the bulk email service, but most will!). Another method is to understand the email it self, bulk email systems will almost always have links to images, and other areas, and most all of them work with legitimate companies, so identifying the email as coming from a real bulk email system will typically give you a real unsubscribe. The rule here is hover and check, and if your still not sure, then don't click, just delete it.

The point to all this is that some simple management techniques can make a huge impact and help remove many threats that come at you.

And paying a little extra for a good anti-virus, with email / internet protection can be another major help. (and more on this… at another time.)