To the Editor March 23, 2020

How to Avoid Ransomware [ran-suh m-wair] noun

Ransomware is malware (malicious software) planted unknowingly in a computer or mobile device that disables its operation or access to its data, until the owner pays to regain control or access. https://www.dictionary.com/browse/ransomware?s=t

Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file, that the user is tricked (see Phishing) into downloading or opening when it arrives as an email attachment. https://en.wikipedia.org/wiki/Ransomware

Organizations in the throes of cleaning up after a ransomware outbreak typically will change passwords for all user accounts that have access to any email systems, servers, and desktop workstations within their network. But all too often, ransomware victims fail to grasp that the crooks behind these attacks can and frequently do siphon every single password stored on each infected endpoint. The result of this oversight may offer attackers a way back into the affected organization, access to financial and healthcare accounts, or — worse yet — key tools for attacking **the victim's various business partners and clients**.

The point here is you could be infected by or have your login credentials stolen by one of your vendors or customers that have been attacked. For example:

-Identity and password management platforms Auth0 and LastPass
-Multiple personal and business banking portals;
-Microsoft Office365 accounts
-Direct deposit and Medicaid billing portals
-Cloud-based health insurance management portals
-Numerous online payment-processing services
-Cloud-based payroll management services
-Prescription management services
-Commercial phone, Internet and power services
-Medical supply services
-State and local government competitive bidding portals
-Online content distribution networks
-Shipping and postage accounts
-Amazon, Facebook, LinkedIn, Microsoft, Twitter accounts

In mid-November 2019, Wisconsin-based Virtual Care Provider Inc. (VCPI) was hit by the Ryuk ransomware strain. VCPI manages the IT systems for some 110 clients that serve approximately 2,400 nursing homes in 45 U.S. states. VCPI declined to pay the multi-million dollar ransom demanded by their extortionists, and the attack cut off many of those elder care facilities from their patient records, email and telephone service for days or weeks while VCPI rebuilt its network. https://krebsonsecurity.com/

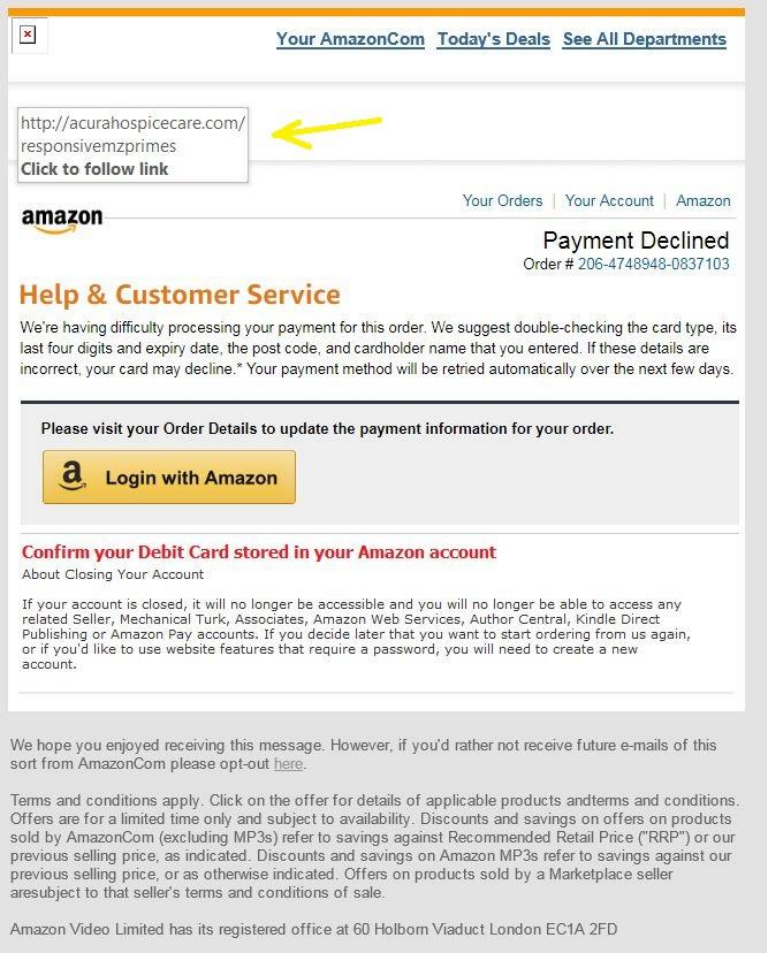
Many times, computer backup files which normally would be used to restore the systems are also effected, meaning encrypted, unless they are disconnected from the individual computers, the computer network, or stored off-site at the time of the attack.

There are many variants of Ransomware including WannaCry, Petya, NotPetya, and Jigsaw. These attacks include a message demanding payment by a date certain, usually in the form of untraceable Bitcoin digital currency. Upon paying, the victim will receive an encryption key to unlock their files. Recently, many

businesses, cloud-computing providers, and municipalities are not paying the ransom and suffering the consequences. To deter this, these bandits are now threating to make public all of the information stolen including documents, emails, and passwords.

If you are a company, hire a vendor like knowbe4.com to train your employees. They will also send out test spam messages and keep track of who the "clickers" are. They will lather, rinse, and repeat, until all the "clickers" are retrained.

If you are an individual, be suspicious of everything. If someone sends you a hyperlink or a button to click on in an email, hover your mouse cursor over it to see where it is going to direct you. If it is not a site you know, don't click! See example below:



Notice that this "follow the link" message indicated by the arrow, is also not a secure encrypted https: address, but a clear text http: address. This is not normal nor acceptable for a payment related service.

How can you defend against ransomware?

1. Update your software. Use anti-virus software and keep it up-to-date. And set your operating system, web browser, and security software to update automatically on your computer. On mobile devices, you may have to do it manually. If your software is out-of-date, it's easier for criminals to sneak bad stuff onto your device.
2. Think twice before clicking on links or downloading attachments and apps. According to one panelist, 91% of ransomware is downloaded through phishing emails. You also can get ransomware from visiting a compromised site or through malicious online ads.

3. Back up your important files. From tax forms to family photos, make it part of your routine to back up files on your computers and mobile devices often. When you're done, log out of the cloud and unplug external hard drives so hackers can't encrypt and lock your back-ups, too.

What if you are a victim of ransomware?

1. Contain the attack. Disconnect infected devices from your network to keep ransomware from spreading.
2. Restore your computer. If you've backed up your files, and removed any malware, you may be able to restore your computer. Follow the instructions from your operating system to re-boot your computer, if possible.
3. Contact law enforcement. Report ransomware attacks to the Internet Crime Complaint Center or an FBI field office. Include any contact information (like the criminals' email address) or payment information (like a Bitcoin wallet number). This may help with investigations.

Should you pay the ransom?

Law enforcement doesn't recommend paying the ransom, although it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. If you pay the ransom, there's no guarantee you'll get your files back. In fact, agreeing to pay signals to criminals that you haven't backed up your files. Knowing this, they may increase the ransom price — and may delete or deny access to your files anyway. Even if you do get your files back, they may be corrupted. And you might be a target for other scams.

https://www.consumer.ftc.gov/blog/2016/11/how-defend-against-ransomware

How to Recognize and Avoid Phishing Scams

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful. The FBI's Internet Crime Complaint Center reported that people lost $30 million to phishing schemes in one year. But there are several things you can do to protect yourself.

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Pay some attention to what you are doing online and you will be fine.