What is ransomware?

Common digital attacks such as malware and ransomware have featured in the news. Here's what you need to know:

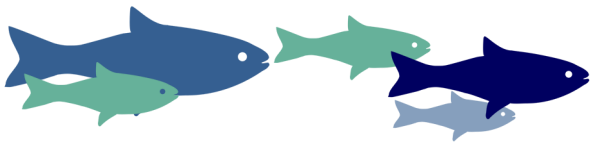
Creators of malware, phishing, and viruses are often motivated by financial or ideological goals. The FBI advises not to pay attackers if they demand payment. Ransomware is the most profitable version of malware according to a 2016 FTC blog post.

Digital files that are meant to compromise a computer or a system take advantage of:

1. Vulnerabilities in software design
2. Mindless clicking of users

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may:

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a "coupon" for free stuff



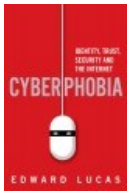
We can fight this

How to Report Phishing
If you got a phishing email or text message, report it. The information you give can help fight the scammers.

Step 1. If you receive a phishing email, forward it to the FTC at **spam@uce.gov** and to the Anti-Phishing Working Group at **reportphishing@apwg.org**. If you receive a phishing text message, forward it to SPAM (**7726**).

Step 2. Report the phishing attack to the FTC website as well at **ftc.gov/complaint**.

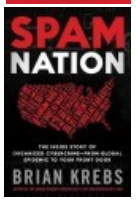
Further Reading



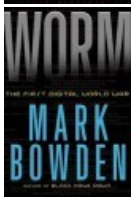
Cyberphobia, Edward Lucas
2015, 364.168 LUC

Future Crimes, Marc Goodman
2015, 364.168 GOO

Privacy in the Age of Big Data, Payton & Claypoole
2014, 005.8 PAY



Spam Nation, Brian Krebs
2014, 364.168 KRE



Worm, Mark Bowden
2011, 005.84 BOW

For more information on online security topics, visit the FTC website:
https://www.consumer.ftc.gov/topics/online-security

The information contained in this pamphlet is taken in part from the FTC website.

EC-7/19

Community Library of DeWitt & Jamesville

Ransomware and Phishing

Protect yourself from common schemes used by criminals on the internet

5110 Jamesville Road
DeWitt, NY 13078
315-446-3578
www.CLDandJ.org

Don’t take the bait

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: **Do I have an account with the company or know the person that contacted me?**

If the answer is “No,” it could be a phishing scam. Go back and review the tips under the header “what is ransomware?” on the inside flap and look for signs of a phishing scam. If you see them, report the message and then delete it.

If the answer is “Yes,” contact the company using a phone number or website you know is real. Do not use the information displayed in the email. Attachments and links can install harmful malware.

What to do if you responded to a phishing email

If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to **IdentityTheft.gov**. There you’ll see the specific steps to take based on the information that you lost.

If you think you clicked on a link or opened an attachment that downloaded harmful software, **update your computer’s security software. Then run a scan.**

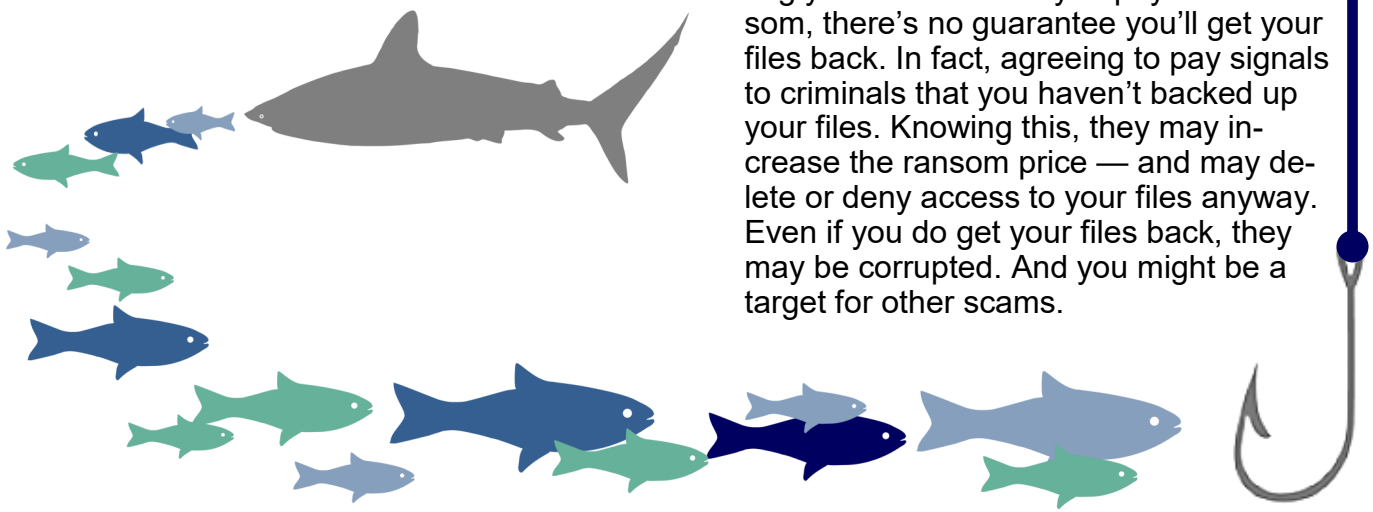
If you think you went to an inauthentic website and entered your login information, **reset your password**; then reset any other passwords on sites where you use the identical password. Only use official login pages to enter or reset your passwords.

Be prepared to recover

Update your software. Use anti-virus software and keep it up-to-date. 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.

Think twice before clicking on links or downloading attachments and apps. According to one expert, 91% of ransomware is downloaded through phishing emails. You also can get ransomware from visiting a compromised site or through malicious online ads.

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.



You’ve been attacked

Contain the attack. Disconnect infected devices from your network to keep ransomware from spreading.

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.

Contact law enforcement. Report ransomware attacks to the Internet Crime Complaint Center (https://www.ic3.gov). Include any contact information (like the criminals’ email address) or payment information (like a Bitcoin wallet number). This may help with investigations.

Should I 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.