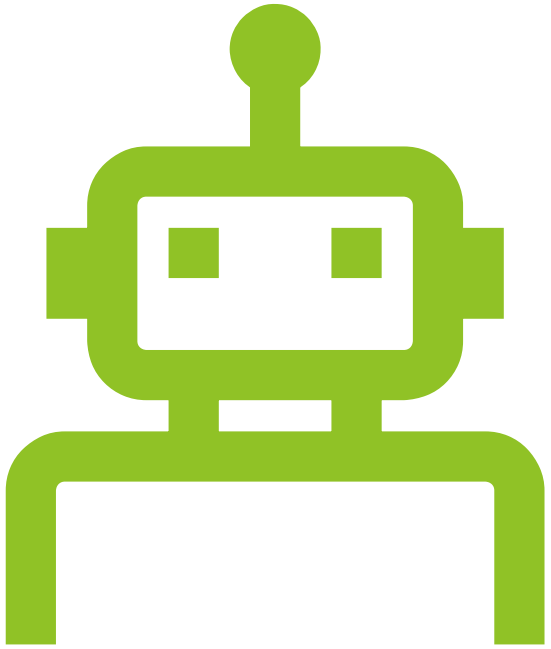


How to Not Get Scammed

Mankato Computer Technology

Scams and Hackers

Malicious hackers are motivated by different things. Some do it for fun, some want money, and others just want to end your business. Getting to know how they behave and what drives them informs how you must defend your organization against them.

Script kiddies

In terms of skill, script kiddies (or skids, for short) are at the bottom of the hacker totem pole. Their name comes from the fact that they use scripts or other automated tools written by others. They are often young people on a quest for internet notoriety or who are simply bored and in search of a thrill.

Script kiddies shouldn't be dismissed so easily, however. The ILOVEYOU virus, considered one of the worst malware on the planet, was developed by skids.

Hacktivists

Hacktivists often hack into businesses and government systems to promote a particular political agenda or to effect social change. These so-called “hackers with a cause” steal confidential information to expose or disrupt their target’s operations.

Even if you’re a small- or medium-sized business (SMB) owner, you’re not immune to hacktivist attacks. This is especially true if your company is associated or partnered with organizations that are prime hacktivist targets.

Cybercriminals

Cybercriminals break into digital systems or networks with the intent to steal, destroy, taint, and/or lock away data. They usually target individuals, SMBs, and large companies that have exploitable weaknesses in their cybersecurity.

Cybercriminals attack using a number of methods, including social engineering tactics to trick users into volunteering sensitive personal or company data. This information is then used for identity theft, sold on the dark web, or leveraged to launch attacks against other businesses. Cybercriminals can also infect computers with ransomware and other types of malware.

State-sponsored hackers

True to their name, these hackers are backed by governments. The hackers' goal is to promote their backer's interests within their own country or abroad. In most cases, this involves taking down websites that criticize the state, swaying public opinion, cyber-terrorism, and leaking top-secret information, among others.

As they are, state-sponsored hackers are already dangerous to business owners, but even more so when they make it their goal to cripple an entire country's financial system or disrupt commodity supply lines. This could involve interfering with the economy or disrupting business operations. Tech and pharmaceutical companies are a frequent target, but businesses in other industries aren't safe from state-sponsored hackers either.

Insiders

The scariest type of hacker is the one that lurks within your own organization. An insider can be your company's current and former employees, contractors, or business associates. Oftentimes their mission is payback. They'll steal sensitive documents or try to disrupt the organization's operations to right a wrong they believe a company has done to them. Edward Snowden is a prime example of an insider who hacked the organization he worked for — the US government.

Malicious hackers are always changing their tactics to meet their goals, making them an ever-present threat to any organization, including yours. It's crucial that you stay one step ahead by working with cybersecurity experts who can help protect your company from dangerous hackers and other cyberthreats. Contact our team today to get started.

-
  -
  -
  -
-
-


Personal
Data

What can be done?

- End User Training
  - Err on side of caution
  - Look for red flags – spelling/grammar, sender domain
  - Check links – hover mouse
  - Pick up the phone
  - Pause before giving out any personal information
  - Serious limitations – bad guys are too smart

What can be done? (continued)

- Best Practice Protections in Place
  - Antivirus
    - Centrally Managed
    - Monitored
  - Firewall
    - Hardware vs Software
    - Subscription service

What can be done? (continued)

- Best Practice Protections in Place
  - Multi Factor Authentication (MFA)
    - Prevents 97% of phishing attacks
  - Monitoring
    - System wide
    - Events associated with a hack
  - Keep systems up to date
    - Windows Patches
    - Network Equipment

The Scam Countdown

- **Tax scams**
- **How it works:** Someone claiming to be from the IRS calls to say you owe back taxes. The caller threatens to arrest you if you do not pay immediately, usually by money transfer or prepaid debit card. The caller ID is spoofed so that the call appears to be from a government agency or the police.
- **How to tell it's a scam:** The IRS never calls.

Debt collection scams

- **How it works:** Someone calls claiming you have an unpaid debt and threatening wage garnishment, lawsuits, or even jail time if you don't pay immediately. The scammer often spoofs the telephone number of a government agency or law enforcement to amp up your fear.
- **How to tell it's a scam:** Debtors have rights and the caller may be breaking them. Be sure to know your debtor rights.
- http://www.consumerreports.org/cro/news/2015/04/protect-yourself-from-debt-collection-scams/index.htm

Sweepstakes, prizes and gifts scams

- **How it works:** You receive a call, letter, or email announcing you've won a prize. However, in order to receive the prize, you must pay a fee for delivery, processing, or insurance.
- **How to tell it's a scam:** You never entered the contest. "You should never have to pay money to claim a prize," the BBB notes.
- http://www.consumerreports.org/cro/magazine/2013/07/gotcha-you-have-not-won-2-million/index.htm

Tech support scam

- **How it works:** A "Microsoft technician" calls claiming to have detected a virus on your computer and promises to correct the problem remotely—for a fee. These callers are actually hackers trying to steal money or use your computer password to steal your personal information or implant malware in your system.
- **How to tell it's a scam:** You haven't had any computer problems. And if you suspect there is a problem with your computer, take it to a trusted repair shop.
- http://www.consumerreports.org/consumer-protection/how-to-identify-a-phone-scam/

Government grants scam

- **How it works:** You receive a phone call, email, or letter saying that you've qualified for a government grant. In order to receive the grant, however, you are told to pay a processing or delivery fee, usually by wire transfer or prepaid debit card.
- **How to tell it's a scam:** You didn't apply for free money. Note, the government doesn't hand out free money that you haven't applied for.
- http://www.consumerreports.org/cro/news/2014/08/watch-out-for-these-impersonation-scams/index.htm

Loan application scam

- **How it works:** While researching loans, you see an enticing ad and click for more info. After filling out the application, you receive an email or phone call saying that your loan application has been approved but you must first send a processing fee, security deposit, or insurance payment. Not only is there no loan but if you follow the instructions, you've shared your personal information, opening yourself up to identity theft.
- **How to tell it's a scam:** Hover your mouse over the link before clicking; if the name doesn't match the company advertising the loan, it's a scam. If you do get scammed anyway, freeze your credit to prevent a criminal from opening new accounts in your name.
- http://www.consumerreports.org/cro/news/2014/02/should-you-put-a-security-freeze-on-the-credit-file/index.htm

Credit card scams

- **How it works:** Someone posing as your credit card issuer calls to say you qualify for lower interest rates, or that he or she needs to verify a recent transaction. The caller asks for your credit card number and security code to “confirm your account details.” In fact, that data is used to steal your identity.
- **How to tell it’s a scam:** A credit card company would already know your number. When someone asks for personal information, they're usually scammers trolling for data.
- http://www.consumerreports.org/cro/magazine/2015/05/prevent-credit-card-fraud/index.htm

Work-from-home scams

- **How it works:** You answer an online ad offering to pay you big bucks while working from home. In fact, it's a front for stealing your personal information from your resume or employment form.
- **How to tell it's a scam:** If it sounds too good to be true, it probably is. Investigate the business before sharing any personal data.
- https://www.forbes.com/sites/groupthink/2011/12/13/16-work-at-home-scams-to-avoid/#b70fba46f650

Fake check/money order scams

- **How it works:** Someone pays you more than you are owed for goods or services and asks you to deposit the check and wire the difference. The check is a fake and when it bounces, you're out the money *and* the fee.
- **How to tell it's a scam:** You are not a bank, so the only reason for someone to ask you to act like one is to extract money from you.
- https://www.thebalance.com/money-order-scams-315055

Photo: iQoncept/Shutterstock.com

Lottery “winnings” scam

- **How it works:** You receive a call, letter, or email saying you’ve won a large amount of money in a foreign lottery. In order to collect it, though, you need to pay upfront for taxes and fees.
- **How to tell it’s a scam:** Such lotteries are illegal. Even if you receive a check as partial payment, the check will be counterfeit.
- https://en.wikipedia.org/wiki/Lottery_scam

10 tips on how to help reduce spam

Don't reply to spam

- Never reply to an e-mail message — not even to unsubscribe from a mailing list — unless you know and trust the sender, such as when the e-mail message comes from a service, an online store, or newsletter that you have signed up with. Answering spam just confirms to the spammer that your e-mail address is an active one.

Take advantage of the Junk E-mail Filter in Microsoft Office Outlook

- Office Outlook helps to mitigate the problem of spam by providing the Junk E-mail Filter, which automatically evaluates incoming messages and sends those identified as spam to the **Junk E-mail** folder.
- https://support.office.com/en-us/article/Overview-of-the-Junk-E-mail-Filter-b62b80c7-1024-4399-98c4-0569eca74e9a?ui=en-US&rs=en-US&ad=US

Block pictures in HTML messages that spammers use as Web beacons

- Office Outlook has an additional anti-spam feature. By default, this feature blocks automatic picture downloads and other external content in messages if the content is linked to a server. If you open a message that has external content when this feature is turned off, the external content downloads automatically, inadvertently verifying to the server that your e-mail address is a valid one. Your e-mail address can then be sold to a spammer. You can unblock external content for messages that come from sources that you trust. For details, see Block or unblock automatic picture downloads in email messages.

- https://support.office.com/en-us/article/Block-or-unblock-automatic-picture-downloads-in-email-messages-15e08854-6808-49b1-9a0a-50b81f2d617a

Turn off read and delivery receipts and automatic processing of meeting requests

- Spammers sometimes resort to sending meeting requests and messages that include requests for read and delivery receipts. Responding to such meeting requests and read receipts might help spammers to verify your e-mail address. You can turn off this functionality. However, read and delivery receipts and automatic processing of meeting requests are useful features that you should not be afraid to use within a secure corporate network.


SPAM

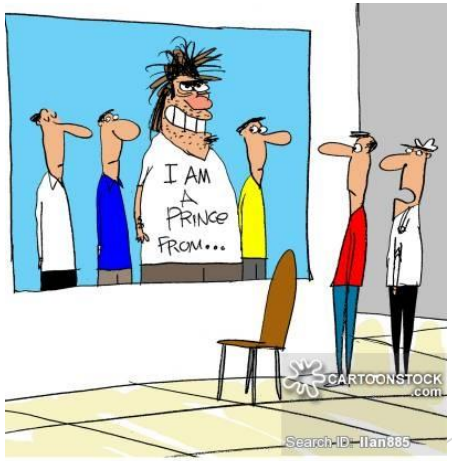
Review the privacy policies of Web sites

- When you sign up for online banking, shopping, or newsletters, review the privacy policy of the site carefully before you reveal your e-mail address or other personal information. Look for a link or section (usually at the bottom of the Web site's home page) called "Privacy Statement," "Privacy Policy," "Terms and Conditions," or "Terms of Use." If the Web site does not explain how your personal information will be used, consider not using the services at that site.

"That's odd, that site verified my age by having me type in all my credit card information."

If a company uses e-mail messages to ask for personal information, don't respond by sending a message

- Most legitimate companies will not ask for personal information to be sent in e-mail. Be suspicious if they do. Such a request could be a spoofed e-mail message disguised to look like a legitimate one. This tactic is known as *phishing*. If the possible spam appears to be sent by a company that you do business with — for example, your credit card company — then call the company to verify that they sent it, but don't use any phone number that is provided in the e-mail. Instead, use a number that you find by using other means, such as directory assistance, a statement, or a bill. If the request is a legitimate one, the company's customer service representative should be able to assist you. The Junk E-mail Filter also includes phishing protection to help identify and disable suspicious messages.
- https://support.office.com/en-us/article/Enable-or-disable-links-and-functionality-in-phishing-e-mail-8c268cc9-7049-419a-b387-4d7932fa6056?ui=en-US&rs=en-US&ad=US



"Okay, sir, can you identify the spam?"


YOU GET JUNK EMAIL. AND YOU GET JUNK EMAIL
EVERYBODY GETS JUNK EMAIL
memegenerator.net

Don't forward chain e-mail messages

- Besides increasing overall e-mail volume, by forwarding a chain e-mail message you might be furthering a hoax — and meanwhile, you lose control over who sees your e-mail address.

My Junk Mail Folder Tips and Tricks

Look

Look if you recognize the person or product.

Verify

Verify that it is a product or service you use.

Verify

Verify the Email address (long strands of numbers and letters aren't legit).

Scan

Scan the content (look for capitalization and spelling errors)

Determine

Determine what to do, Block, Delete, move to inbox


camalot

Conclusion

- How do I keep my business safe?
  - Work with a professional IT company
  - Implement best practices
  - Train staff
  - Plan for the worst

Scam a lot videos on YouTube


M
TOASTER
SCAMALOT

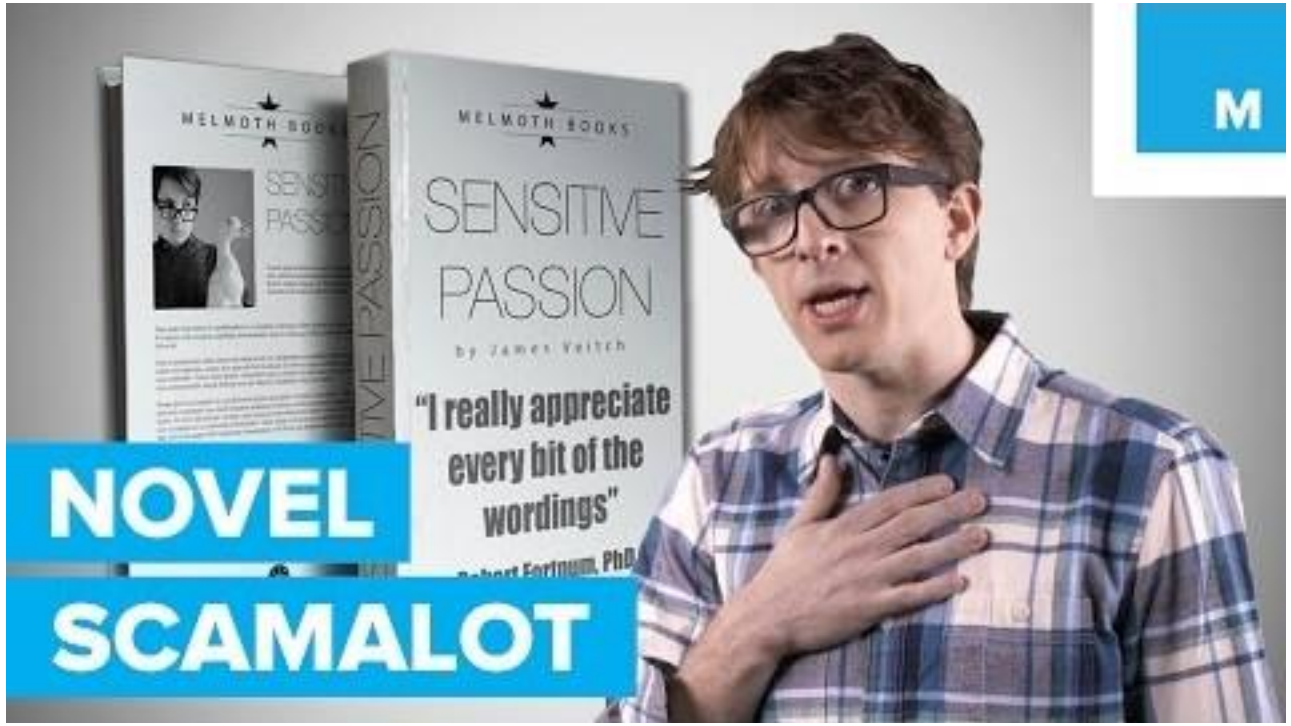

M
GOLD
SCAMALOT


PASSPORT
United States of America
HONG KONG
SCAMALOT


M
WINNIE
SCAMALOT


SNAIL PARK
SNAIL FARM
SCAMALOT
M


M
POISON
SCAMALOT


MELMOTH BOOKS
SENSITIVE PASSION
by James Veitch
"I really appreciate every bit of the wordings"
NOVEL
SCAMALOT