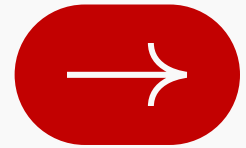


SCAM TACTICS

---



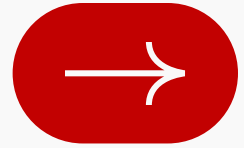
# Layman's Guide to Scam Tactics

Read to avoid falling prey. Share to spread the word.

---

[KirkhamIronTech.com](http://KirkhamIronTech.com)

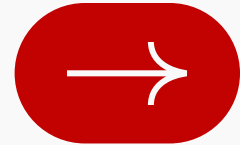
**KIRKHAM**  
**IRONTECH**



# Phishing

Scammers systematically create fraudulent services and businesses in order to scam unsuspecting victims. They harvest email lists in masse and spray them with more or less convincing messaging to see who bites.

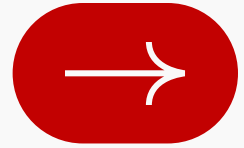
**Those who open, respond or engage with those generic emails are now targets.** Hackers then hone in on their target to create an extremely tailored, subtle approach. As soon as you receive and open a suspicious email, alert your email provider, block the sender's domain and inform your IT person.



# Spearfishing

A sophisticated, laborious method whereby hackers harvest private data from social media or other data breaches and shortlist specific high value targets. They pour over details of the targets' lives to simulate an affinity with them. These attacks are so subtle they can go undetected for weeks or months because of how similar they are to **real-life communication**. It starts out as a con that ends in an attack - ransom, kidnapping, blackmail. Nothing is off limits.

If you are a high net worth individual, you must take extra precautions. **They might already be watching.**

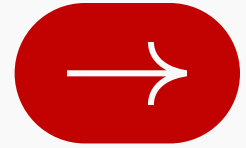


# Smishing

A portmanteau of **SMS + phishing**. Smishing attacks consist in communication that could easily pass as a real SMS text from an individual or business.

The number the SMS is sent from might even be listed as a legitimate organization.

The dead giveaway is receiving an SMS or iMessage **asking for your password**. Do not share your passwords with anyone for any reason. Do not click on any links in SMS messages. It's a scam.

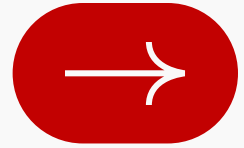


# Vishing

A new or unknown caller from an organization that you already trust will leave a **voice mail message** asking you to call them back with personal information.

When a company you trust has a data breach, hackers now have your contact. They will impersonate businesses you already know to gain your trust.

Before responding, check with the business they claim to be. **You lose nothing by being vigilant.** Avoid imposters.

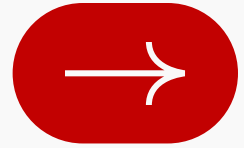


---

# High pressure language

One of the reasons scams are so successful -- according to the **FBI \$1.2B are stolen annually via cybercrime** -- is because the perpetrators create a sense of urgency in their victim by using high pressure language.

The best way to detect this manipulation tactic is by noticing your own physical and emotional response to a message. Do you feel urgency? Check in with yourself before taking action. Hackers leverage your stress to benefit from poor decision making.

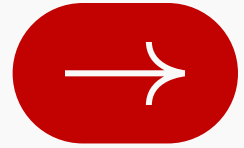


---

# Data Manipulation

Your company has **at least one highly sensitive database** containing financial records, passcodes and/or confidential client information with access restricted to specific highly trusted individuals.

A data manipulation attack takes place when a hacker gains access to that database and **tweaks it from the inside** to create additional logins to intercept that information -- even in secret, without anyone ever knowing. Until it's too late.

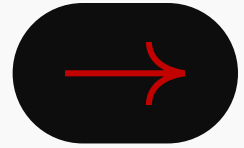


# Baiting

Is the subtle art of enticing you to interact with a scam through social engineering. The three elements that pique curiosity and enhance social influence are: the **mysterious**, the **unfinished** and the **self-relevant**. A mystery component in any phishing email receives 7x more clicks on average.

If you receive messaging via email that almost seems *too interesting*, be suspicious.



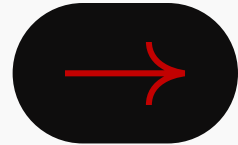


# Watering hole attacks

Most teams have a set of websites or services they frequent often in order to communicate or work on a task. That is the proverbial **digital 'watering hole'** for that group.

A watering hole attack takes place when hackers target a specific group of end users within an organization by baiting them using *spearphishing* attacks via their **realm of influence** aka their watering hole.

There is also the chance cybercriminals will infect a watering hole with **malware**.

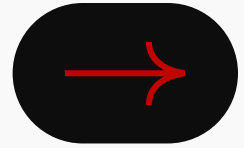


# DNS spoofing

Domain Name Server (DNS) spoofing (a.k.a. **DNS cache poisoning**) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

In this type of attack the URL you typed in takes you to a lookalike site you don't want to be visiting, in order to steal your login credentials. **Stick to your gut.**

The best way to avoid this scam is to avoid clicking on suspicious links from mystery senders and always check that the URL starts with **https://**



# Pretexting

If you receive an unexpected email from a high status individual within your organization, your first reaction might be excitement or nervousness followed by the desire to **please and impress** them by complying with their requests. Hackers know that.

They use this technique to **impersonate C-suite and other executives** and gain access to confidential information from other employees. That is a prime example of a whaling attack based on pretexting. It's horrifically effective. Stay vigilant.

---

# Was the Layman's Guide to Scam Tactics helpful?

Please feel free to send us an email with questions or comments. Spread the word and forward our guide.



**INFO@KIRKHAMIRONTECH.COM**

[www.kirkhamirontech.com](http://www.kirkhamirontech.com)



---

**479-434-1400**

**INFO@KIRKHAMIRONTECH.COM**

**SCHEDULE A MEETING WITH US! [HTTPS://KIRKHAMIT.AS.ME/DAVIN](https://kirkhamit.as.me/davin)**