5 Big Cybercrime Trends of 2019

Fraudsters got more sophisticated…and so did we.

Personalized Fake Emails and Texts

Think about all the personal information you post on Facebook, LinkedIn and Instagram. Crooks do. They scan social media comments and send personalized phishing emails and texts that look convincing. At first, they targeted CEOs, instructing them to wire "past-due" payments. That worked so well, scammers targeted others in leadership positions. Then this year, they expanded their schemes to include rank-and-file employees. **Remember, if you receive an urgent email or text at work with a personalized message instructing you to click on a link, download an attached PDF or Word document, wire money or send gift cards, trust your instinct and be suspicious!**

Dangerous Power Cables and Plugs

Hacking technology has become so advanced, crooks are using charging cables and fake charging stations that record keystrokes that victims type on their smartphones and tablets. These cables and power outlets look exactly like the ones that come with phones. But embedded in one end is a tiny device that records passwords, texts and emails. The fake devices then transmit data back to the crooks who use it to access private information stored on the device. Mass production of these dangerous cables and plugs is now underway, so fake cables will be an even bigger problem in 2020. **If you find a charging cable on the ground, in an airport, coffee shop or other public places, don't plug it into your phone or tablet.**

Phony Website Addresses

This holiday season, there are four times as many fake stores claiming to sell merchandise on the web as there are real stores! Some sites sell counterfeit merchandise and others exist just to steal credit card information. Many fake sites use web addresses that are close to familiar addresses except for substitution of a random letter like a "0" instead of an "O". Others use a name that's close to the real thing like "amazon-deals.com" instead of "amazon.com. Most claim to offer super low prices on popular items like fragrances, sporting goods, Ray-Ban sunglasses and shoes but only accept PayPal as payment. **Before you enter your credit or debit card information online, be certain that the retailer is legitimate and double-check that the web address is what it should be.**

Threatening Robocalls

This year, because phone technology has become so inexpensive, the number of robocalls in the US jumped to nearly 2,000 per second. Many fake calls follow this format: the urgent recording on the other end claims to be from the IRS, social security administration, the FBI or local police department. If you remain on the line, a real person takes over and threatens you with a steep fine, arrest and jail time if you don't comply with their instructions immediately, which usually involves sending them money in the form of gift cards or wire transfers to a "secure" bank account, usually located overseas. Robocalls are common because so many people take the bait and send fraudsters money. **If you receive a threatening call, simply hang up. Government agencies and law enforcement won't make threatening phone calls instructing you to pay money or provide personal information over the phone.**

New Privacy Protection Laws

If you're like most people, you click "Accept" when a website asks you to approve the way they collect and use your personal information. The US doesn't yet have a national privacy law to govern how that information is used. As a result, states are creating their own regulations that govern how long companies have to alert their customers to a security breach, how consumers' information is bought and sold, and the consequences when a consumer's information is stolen. **Watch what happens to privacy laws in the upcoming year. California, New York and even Nevada are moving to put strong regulations on the books designed to give you more visibility and control over your personal information.**

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION