The New Face Of Fraud in 2017

February 21, 2017

Fraud, identity theft, and other scams are very prevalent in today's digital world. In 2017, here are some major developments that we should keep an eye on.

Identity theft and other forms of fraud are increasingly common today, and most people would like to think that they know how to protect themselves. Unfortunately, as individuals become savvier about technology use and privacy protections, the thieves behind these crimes also get smarter.

In 2017, expect to see new forms of fraud pop up, including strategies like “typosquatting,” affinity fraud targeted through community or cultural groups, and more dangerous types of malware, among others.

Here’s what you need to know to prepare yourself.

That’s No Mistake

Most people have an occasional typo when entering their account information on websites, but it's more important than ever to be sure whether or not you made a legitimate mistake. Typosquatting is a new form of identity theft and is premised on mock-ups of authentic sites and false typos.

What does this look like in practice? You’ll receive an email that, like so many other fraudulent messages, looks as though it came from the real company. If you follow the sign-in link in their email, however, you’ll arrive at a fake site front and when you log in, the site will redirect you, stating that you made an error while signing in.

Of course you didn’t make a typo, but by now it’s too late – the fake site has stolen your login credentials and can now access your account. The redirect, however, will be to the real site. This can make it even harder to detect such a scam.

As always, be suspicious of emails from retailers or banks and never click internal links. If you need to access a site to deal with a problem, enter the URL yourself and navigate to the correct part of the site or use a bookmarked version of the page.

Fraudulent Friends

One popular form of financial appeal is that which is based on affinity – you see it all the time. You get a letter from an organization claiming to be affiliated with your regional or religious community, or another group you belong to, and they’re asking for money or proposing a kind of investment. Before you hand over the money, though, take a second to assess the organization.

Affinity fraud relies on the belief that because you are supposedly connected to this group, you won’t do your due diligence. The organizations aren’t real and they will take your money and disappear. Before you write that check, look into the organization to make sure they really represent your community.

Taken For Ransom

Malware has always been a problem for computer users, but in the past it typically did things like crash your computer or spread a virus through your email. Now, however, there’s a type of malware known as ransomware that can take your devices hostage – and it doesn’t discriminate. One form of ransomware attacked hospital files, and you can expect that more of these programs will come after personal accounts and devices.

Remember, the more accounts you secure with the same password, the easier it will be for malware of this type and other cyber thieves to take over your accounts. Vary your passwords and change them regularly. This will reduce your risk of account takeovers.

Be Alert, Be Prepared
In the face of more adroit digital fraudsters, it's important that individuals be more tactical than ever in their approach to personal security. Download and update your antivirus software, change your passwords, and be careful using public wifi networks. If you have a business, look for programs that can detect check fraud and encrypt all of your files.

Digital fraud demands high-tech precautions in equal measure. Be prepared.