Guarding You Against Technology's Dragons

afl's Knights of Technology, LLC
4072 Foxpointe Dr.
West Bloomfield, MI 48323
jeff.lipshaw@aflcc.com
248-215-0895

INFORMATION TO SHARE TO PROTECT AGAINST HOLIDAY SCAMS

1) IRS, police, local governments, the courts, etc. will not contact you by phone. They always contact you by mail.

2) No company that you might owe money to will ask for you to pay it by going to the store and purchasing gift cards of any sort. Once the code is given off the back of the card, the money is gone.

3) If you have an issue with any technology, be very careful looking up the contact information on the internet. Often, the first information that comes up is a paid ad and isn't really for the true company. They just want to get access to your computer, credit card, banking information, etc.

4) Anytime you are asked to send money to get money, it is a fake scheme. Remember, if it sounds to good to be true, it probably is.

5) Be careful of any site that you are choosing to purchase holiday gifts from. If you have never heard of it, then you should confirm the country it is based out of and what others have to say about it (and not from the site itself). If it is outside of the country, you will be charged a fee

6) When going to use your credit / debit card anywhere, especially at gas stations, grab the place you are to slide the card into or though and make sure it doesn't move or separate from the rest of the scanner. If it does, then there is a skimmer attached and if you use it your cards information will be sent off to a hacker

7) Microsoft nor any other company is monitoring your computer unless you are paying them to monitor it. If they call and get you to look at something on your computer that they can tell you the information about. That information is the same on all computers. They don't really know anything about your computer. They just want to get on to steal passwords.

8) If you receive an email that your password has been hacked for any service that you use including your bank, aol, gmail or any store. Don't click on the link in the email to go to change your password or to log in to confirm your login credentials. Go to that site the normal way you do and check it, call the company directly about it if you have their phone number (like on the back of a bank statement or credit card) or share it with whoever helps you with your computer to have them confirm if it is legit or not. This is normally just another means of trying to get your login and password.

Guarding You Against Technology's Dragons

afl's Knights of Technology, LLC
4072 Foxpointe Dr.
West Bloomfield, MI 48323
jeff.lipshaw@aflcc.com
248-215-0895

9) If you receive an email showing your password (or a password that you used at some time) claiming that they have hacked into your system and will share your information, etc. if you don't pay them some bitcoin don't do it. This is a fake. What has happened is that password was stolen and was found on the dark web and they are trying to use it to get money from you. What you need to do is make sure to change any place that you use that password to a new password and never use that password again. You might also want to have someone check the dark web for you to see what other information is out there.

10) The same goes if you get an email claiming that they were watching you doing things on porn sites. They know that many people go on porn sites so use it to just scare you into paying them money, again bitcoin. But, it isn't real. If it was, they would include a picture. This is also a reason that people purchase covers for their webcams, just to help make sure no one can watch them without them knowing.