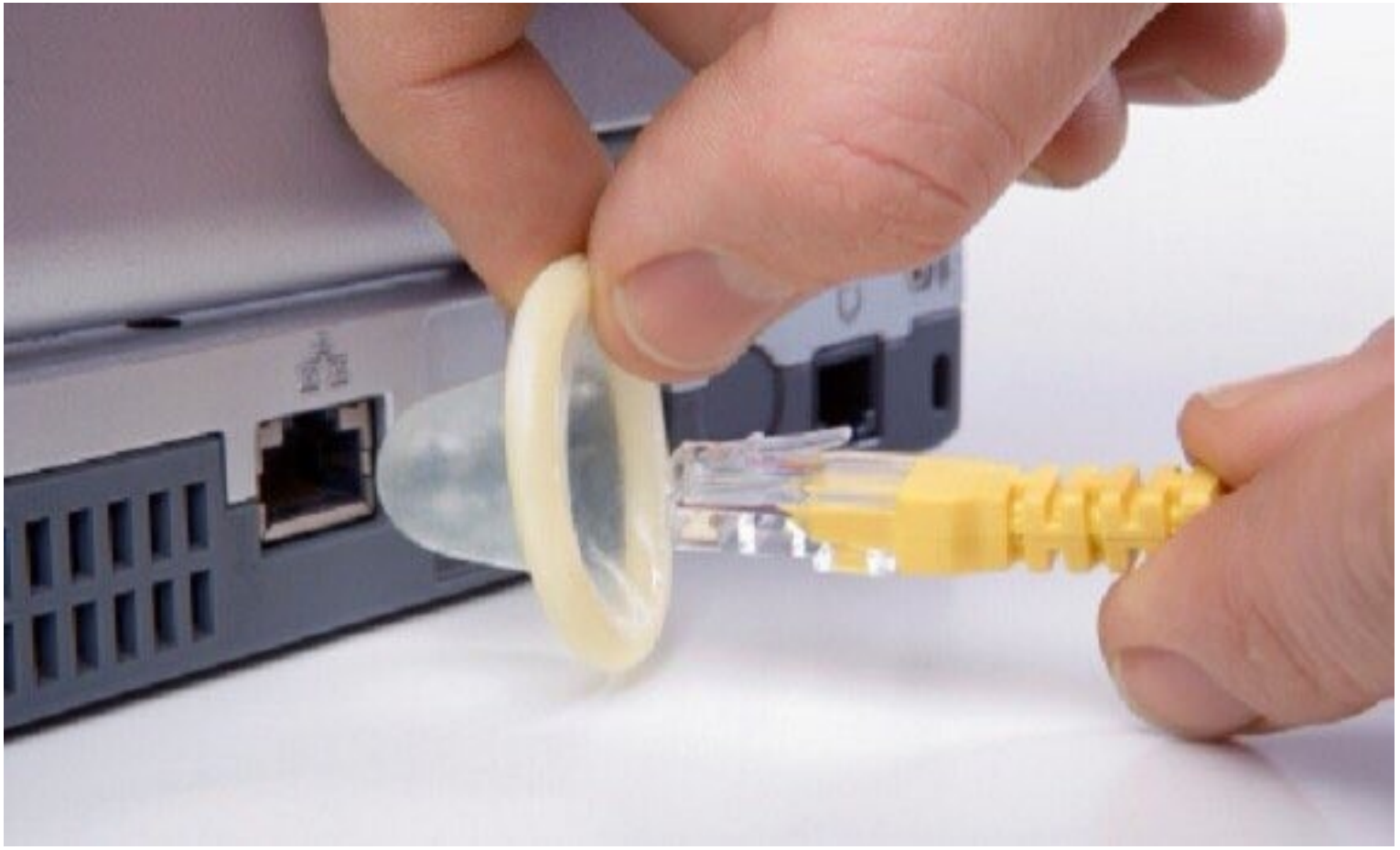
Internet Safety

What the Heck is Internet Safety?



Internet safety or online safety or cyber safety or E-Safety is trying to be safe on the internet

It is the act of maximizing a user's awareness of personal safety and security risks to private information and property associated with using the internet.

It is also the self-protection from computer crime.

Discussion Topics

- E-Mail Scams
- Social Network Scams
- Viruses, Key Loggers, Root Kits, etc.
- Tips for Staying Safe
- Final Thoughts

E-Mail Scams


ROYAL BANK
of
NIGERIA
I have emailed everyone
I can possibly find, my Prince,
but no-one wants to help
you move your money.

Common E-Mail Scams

- Nigerian Prince – still active. These days he is usually a Swedish widow or a British orphan. This scam is pre-internet and was originally known as the Spanish Prisoner.
- Phishing – one of the most popular. Scammers want to get network access to corporations, hospitals, schools, etc. First known phishing scam was on AOL.
- Credit Cards – it the bank doesn’t need to verify your data, some company is offering a low interest no fee card that you need to pay to activate.
- Disaster Relief, Ransomware, Free Vacations, Sweepstakes, and thousands more.

Social Network Scams

Not surprisingly, most scams and hoaxes on Social Media Sites were originally e-mail scams.

Just like that Nigerian Prince, Mark Zuckerburg isn't really going to give his millions away to thank all of his faithful Facebook users.

Let's review some other common (mostly Facebook) scams.

The first 500 people to share this post will win a free iPhone, gift certificate, RV, television, or something equally valuable

Sorry, but you were number 501. You just gave some information to the scammer. There is a good chance that you also gave information about your friends.

1000 likes isn’t really going to get some child in Africa a much needed operation.

Once there are enough likes, the post’s popularity soars. The original poster can then change the content and replace it with something else – usually some kind of malware.

This is called “Link Farming”

Only a genius can find the 5 among all the S's?
Are you smart enough to find errors in a picture?
Can you find the word "tiny" in this maze?

All of these "brain" games really show how stupid people can be when they play them. The designers are likely just gathering data.

I've noticed that many people who share these posts often get a "virus" from somewhere.

Why do scammers want you to "copy and paste" instead of "share"?

1) This creates a new instance of the message. If the original message gets deleted, the copy and shares still exist.
2) Then all your friends will see it. If they do the same more and more people make start posts.
3) This makes it much harder to track the original poster.

Viruses, Key Loggers, Root Kits, etc.

Less common in recent years, but still found.

- Usually come in program files
- Can be embedded in any file
- Can be installed be web sites without warning
- Often come in unsolicited e-mail links

I’m sure no one in this group would fall for this!

Why Are There So Many Scams?

- Because they work
- Like Fox Mulder, people want to believe
- They all look so good
- Many people are just goodhearted
- They are easy for the con artists to use
- They are easy to constantly evolve

Tips for Staying Safe

Never Click A Link You Didn't Expect

This especially includes links from people you know. E-mail is easy to fake. The link I sent shows a classic example.

- This is the first time I've ever sent an e-mail like this. Just a link with no explanation.
- Mousing over the link gives you clues. The link goes to a page I named "tricklink".
- I could have easily included bad things on the page. That's how the bad guys work

Don’t give your username or password to anyone.

With your username and password, someone can post language that gets you expelled a site, in trouble with your spouse or even in trouble with the law.

Keep your name and password private

Keep Your Browser(s) Updated

The bad guys can exploit a browser with minutes of a vulnerability being found.

Practice Safe Browsing

You wouldn't choose to walk through a dangerous neighborhood. Don't visit dangerous neighborhoods online. Cybercriminals use lurid content as bait. They know people are sometimes tempted by dubious content and may let their guard down when searching for it.

Don't even give the hackers a chance.

Be Careful What You Download

A top goal of cybercriminals is to trick you into downloading malware or try to steal information.

Don't download apps that look suspicious or come from a site you don't trust.

Be Careful on Public Wi-Fi

Everyone knows this. Many disregard it.

Final Thoughts

- I’ve barely skimmed the surface. There are many other scams.
- Watch the X-Files for advice.
- Follow your intuition. If something feels bad, there is a good chance it is bad.
- Have fun on the Internet, but wear your safety belt.

Next Week

Talking Turkey on the Internet

Some fun Thanksgiving Sites


Thats all
Folks