Inside this Issue Vol 3. Issue 3/19

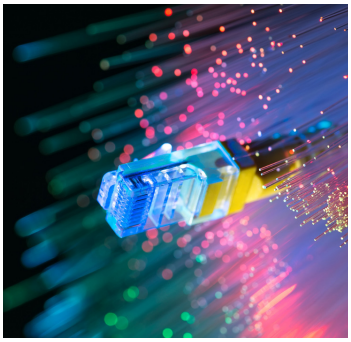
Cyber Tips

How to stay safe on line.

Cybercriminals have become quite savvy in their attempts to lure people in and get you to click on a link or open an attachment.Read more >>

Securing your devices

According to ABI Research, there will be over 30 billion devices connected on the Internet by 2020. Today, our everyday devices are connected to the world



Institute Of Forensics & ICT Security www.forensicsinstitute.org

Forensics & **Cyber Security** Newsletter

Your source of forensics, security and fraud insights

PHISHING SCAMS: Phisher men are closer than they appear

Of recent, phishing is becoming more common and more sophisticated. A recent Microsoft Security Intelligence Report states that phishing attacks are by far the most frequent threat to cybersecurity.

Cyber attackers can credibly impersonate people and email domains, lure victims with fake links, prey on the emotions of people, and craft email attachments that look like what you may expect to receive. Statistics show that one out of 101 emails are malicious and

Security tips

01

Setting strong passwords on your apps will make it harder for a hacker to guess them. It's also suggested to set a different password for each app.

02

Beware of Downloads

When you are downloading apps, be sure to download them from the official app stores and check reviews. Cybercriminals create rogue mobile apps that mimic trusted brands in order to obtain users' confidential information

From page 1

Unsecure devices also give malicious users the means to propagate their attacks onto others by using your insecure devices to attack other networks and devices.

email continues to be the number one threat vector for cyber-attacks. In the attempt to stem the flow of phishing emails, companies have implemented security filters, but on average, more than 14,000 malicious emails per customer per month that get past security filters.

In addition, there are more phishing attacks that are designed to thwart multifactor authentication (MFA) protections. More organizations and individuals are embracing MFA as a means of stopping cybersecurity attacks that seek to compromise credentials. MFA incorporates an additional layer of authentication, rather than just a simple username and password. For example, an SMS-based verification code is sent to the end user's verified mobile phone.

According to security specialists, cybercriminals are incorporating mechanisms in their phishing schemes to capture and instantly use the combination of username, password, and a verification code.

The attackers have adapted to SMS-based verification as part of the authentication process and have built detailed login pages that look like the original page to accept the additional information. Phishing scams are becoming more dangerous and more accessible to unsophisticated operators. The hacker trying to steal your information does not have be a skilled cybercriminal.

Attackers also take advantage of current events to tempt people who are interested or affected by a current situation. For example, the recent Boeing 737 Max plane crash, the Notre Dame fire, champions league games, among others.

The biggest problem with internet users today is that they don't have a definitive perspective about cyber security. Organizations and individuals should be thinking about cybersecurity as an onion. Technical controls such as spam filters, anti-virus (AV) and MFA are layers of the onion that can be used to help protect the core – our data.

However, without end user awareness, any technical control can be defeated. So, what can you do? Be cautious of email messages with the following characteristics:

- Addressed to undisclosed-recipients.
- The from and the Reply-To addresses are different.
- Requests for personal or sensitive information.
- Promises of money or deals that are usually too good to be true.
- Threats or alarming messages.
- Random capitalizations, odd punctuations, misspellings, and improper grammar.
- Message is unexpected and/or out of character from the sender.
- Link in message will take you to a different address than the one that is displayed. Be sure to hover of link to see where it will go.

Security tips

01

Keep sensitive files off your phone

Even better than encrypting your SD card is to make sure the files are never on your phone in the first place. There is no reason these files need to be on your phone when editing them though.

02

Set up a SIM lock

On top of securing your phone, make sure that you've locked your SIM if this is important to you. This is because it requires you to input a PIN before you make a call or send a message, vital if you want to ensure that thieves can't run up massive bills. It's not the most efficient way to use your phone, but if you're in a place that worries you, head into your security settings to enable it.

Securing your devices

Man is not an island, and as such we seek to interact more and more with each other. This has led to a level of intercommunication through the internet that hasn't been seen before. According to ABI Research, there will be over 30 billion devices connected on the Internet by 2020. Today, our everyday devices are connected to the world including laptops, mobile phones, fitness trackers, smart televisions, home security systems, thermostats, and refrigerators. Furthermore, it's important to note the devices that connect everything else together, such as routers, access points, and modems.

Many people may not consider their connected devices to be a security threat, but that is not absolutely true. One of the issues with such devices is that many of them do not come configured with security in mind. This makes it very easy to connect an unsecure device to your network thereby giving attackers access to your personal information.

Manufacturers develop products to be more accessible, more user friendly, and to make our lives more integrated. Nevertheless, that also means we are less secure if these devices are not properly configured. Unfortunately, some devices completely lack the option or ability to configure them, making it nearly impossible to secure them. Unsecure devices also give malicious users the means to propagate their attacks onto others by using your insecure devices to attack other networks and devices.

Therefore, not only can your unsecure devices present a risk to you, but they can also become a risk to others who can be victims of an attack from your compromised devices. Think of this in a normal working environment with such devices on company networks.

Visit www.forensicsinstitute.org/securing-your-devices/ to read full article

Institute of Forensics & ICT Security
Forensics. Security. Training

CERTIFIED FRAUD FORENSIC PROFESSIONAL

ENTRY-LEVEL | 40 HOURS | FEES Tution + Exam **$900**

www.forensics**institute**.org

CFFP is the world's most comprehensive fraud investigation using forensic science. A CFFP can handle any kind of investigation covering digital and financial forensics as well as criminal investigations involving fraud. Fraud Examination is just but a fraction of the CFFP's skills set.

CFFP
CERTIFIED
FRAUD
FORENSIC
PROFESSIONAL

With Practical Skills, You Succeed

IFIS is accredited by the **National Council for Higher Education (NCHE)**