



October 2009

Never email or share your password

There have been a number of recent spam emails claiming to be from KCTCS asking users to reconfirm their account by sending back their password or other personal information. If you have sent your password in any email recently please **change** your password immediately.

FAQ: Don't Click on 'Malvertising'

Instead of hacking into major online sites to embed malware, hackers have found an easier route: walking right in the front door by exploiting security holes in the systems that deliver advertisements.

With "malvertising," also dubbed "scareware," a growing problem, we'll take the opportunity to answer frequently asked questions about this growing threat.



Q: What exactly has been happening?

A: You're web-surfing around, and suddenly - perhaps out of nowhere, or perhaps because you click your mouse - a popup appears. It has some sort of frightening warning that your PC security has been compromised, and advises you to click OK to scan your machine.

Q: What's wrong with this type of ad?

A: Several things. First, it's intentionally designed to look like a Windows popup, rather than an advertisement. Second, it hasn't detected anything at all; it's just an effort to sell you something you probably don't need. Finally, many scareware popups actually point you to malware sites, adding insult to injury.

Q: Aren't ad scams like this a problem only at shady websites featuring porno or gambling?

A: Unfortunately, no. In fact, the current furor was caused when the New York Times website began presenting a scareware popup. Newsweek and the Philadelphia Enquirer are among the other mainstream sites that have run scareware "ads."

Q: Don't they know better?

A: They should, and for the most part they do. For example, the Times was victimized by scammers who initially posted a legitimate ad, then pulled a switcheroo. Remember, though, that old-line newspapers and magazines are in a total fiscal collapse, and thus may not be as choosy as they once were when it comes to accepting advertising.

Keep Your Guard Up When Using Facebook, Twitter

Cyber criminals are finding new ways to use social media and communication websites such as Facebook and Twitter. If you're not paying attention, it's easy to get taken. Here are some tips to help you stay safe:



☒ Don't be fooled by shortened URLs. Twitter limits posts to 140 characters, so shortened web addresses are common. Unfortunately, most users click these tiny URLs without having any idea where they lead - and thanks to hackers, they often lead to IP theft and malware sites.

☒ Beware "friends" in need. Unsurprisingly, criminals are stealing Facebook login credentials. They then send messages to your contacts, pretending to be you in need of money. Double-check all such requests!

☒ Watch out for applications. Facebook applications make the site more entertaining, but they pose an unexpected risk. These applications can access your profile, and the developer can read your wall posts or collect your contact information. To prevent this, only install verified applications. These have a green checkmark in the application directory.

☒ Bad ads. Advertisements on social networking sites are much like newspaper classifieds in that they haven't been vetted. So products may not work as promised, for example, or ads may tout sham work-from-home opportunities.

☒ Quizzes and games. Everybody knows a few Facebook users who seem to feel a pressing need to take every single quiz that comes along. Not only is this annoying, it can trick users into revealing personal information. For example, a quiz involving your mother's name and your pet's name gets you to reveal this info - which is often used as questions when people forget computer passwords, and thus may be of use to identity thieves.

How Would You Fare in a Social Engineering Attack?

As most folks know by now, social engineering uses computer security cracking techniques that rely on weaknesses in human nature, rather than weaknesses in computers or networks. Using social engineering, even an attacker with minimal computer hacking skills can find his way into a supposedly secure computer system and access, modify, or destroy the data in it.



How would you fare if a skilled social engineer took you on? The answer lies in the following question, which are not a quiz, but rather a way for you to understand your own tendencies:

1. Would you give your password to someone who told you in person, over the phone, or in an email message that he was fixing a problem with your computer or network? Or would you notify your computer security personnel immediately?
2. Do you lock your workstation before you leave your desk, or do you leave it up to your password-protected screensaver to activate on its own?
3. Do you challenge strangers you come across in restricted areas who don't display proper badges or identification, or do you assume they're authorized to be there (and perhaps are too important to be questioned - possibly because they're dressed in suits)?

4. Would you decline to participate in a phone survey asking questions about your organization's computers, or would you be likely to participate if offered a free gift?
5. Would you challenge a clean-cut uniformed delivery person carrying packages who asked where the mailroom was, or would you hold the door and point the way?

You can probably see where these questions are leading. There are so many situations in which courtesy and the human desire to be liked point you in one direction - but security points you in the other!

[Spear Phishing: Mini Case Study](#)

A sophisticated email scam cost a Maine business \$150,000 and potentially exposed hundreds of customers' banking information after a company employee fell victim to a cunning phishing attack.



The breach occurred when someone gained unauthorized access to one of Downeast Energy's bank accounts. "We were duped," admitted Downeast Energy president John Peters. "It sounded like, and looked like, an official communication from our bank saying they were updating their information and we had to log on using our user ID and password." The employee who believed the email to be legitimate responded with the information.

Such an attack is called "spear phishing" because rather than sending a generic spam to millions of consumers, the perpetrators narrowly select recipients - in this case, business customers of a particular bank.

What happened next is a worst-case scenario: the perpetrators transferred about \$150,000 out of the account before activity was halted. Even worse, because the account in question was used to hold automatic payments from about 800 customers, it included limited information about them.

Downeast Energy notified those customers, but Peters and law enforcement officials believe Downeast Energy itself was the target of the attack.

[Savvy con artists](#)

Financial regulators say the breach points up a serious problem for businesses and consumers: phishers' level of sophistication grows every year. Analysts report it's not unusual to see supposed bank websites that are complete fabrications. They're very convincing, right down to the "secure key" browser indications that all is well.

Downeast Energy's John Peters says the lesson learned in this case is clear: "The takeaway is that we just constantly have to be vigilant, and no matter how official-looking these communications are, we have to have better systems in place so that no one will respond to a request like that without getting authorization from a higher level."

[3 + 6: Things You Should Know About Wi-Fi Security](#)

These days, a huge number of computer users take advantage of the wireless networks that have sprung up in airports, cafes, hotels, business centers, and just about everywhere else.



But Wi-Fi carries risks as well as data, and the more you know about those risks - and how to avoid them - the better off you'll be.

Risks

1. "Evil twins." Some Wi-Fi networks appear to be legitimate but aren't. Criminals create dummy networks or websites that contain the name of a legitimate airline, hotel, or airport - but actually direct your information to their own computer.
2. Eavesdroppers. It's extremely easy for hackers to intercept unencrypted Wi-Fi transmissions in cafes, hotels, and even in their cars outside office buildings.
3. Everyday security risks. Mobile PCs are vulnerable to the same viruses, Trojans, and worms as your home computer. Many users forget this because they're so focused on wireless-specific challenges.

Protect yourself

1. Assume that others in cafes, hotels, libraries, airports, and other public places can access any information you see or send over a public wireless network.
2. Don't connect to unsecured wireless networks. Remember, if you don't need a password to connect, the bad guys don't either.
3. Make sure your computer settings don't allow automatic connections to hotspots.
4. Use a software firewall. Personal firewall software should be installed and working on your computer.
5. Disable file and printer sharing; these features let other computers on a network access resources on your computer.
6. Take sensitive information that you won't be needing off your laptop altogether before you go on the road.

Computer Viruses 101: Where Do Viruses Come From?

Everybody knows viruses are to be avoided, but did you ever ask where they come from in the first place? We'll address the issue by answering some common questions.

Q: Let's start with geography: Where do viruses physically originate?

A: We're number one! The U.S. has the dubious distinction of providing more viruses than any other nation - 15.9%. Brazil is second, at 14.5%, and Korea makes the podium with 6.2%.

Q: Who actually creates these things?

A: That's the deeper question, isn't it? The answer is straightforward: Behind every virus is a computer programmer who felt the need to create ... a virus.

Q: But why?

A: A variety of reasons. Some hackers want to demonstrate skill. Often, the perpetrators are eager students seeking admiration from their fellows. But more often than not, today's viruses are created by cyber-criminals.

Q: And their goal is profit?

A: Yup. The viruses are designed to steal or copy your personal data for financial gain. The goal may be to access passwords or credit card details; to use your Internet connection for illegal



purposes; or simply to bombard you with spam and bogus advertisements.

Q: How do I steer clear of viruses?

A: The most common source of virus infection is, of course, the Internet, but that doesn't mean you need to stop web-surfing. Most people who do unknowingly catch viruses from the 'net do so because they're click-happy - that is, they will click around and download virtually anything without knowing whether or not they can trust the source.

Here's a simple tip: Before you click on a link, check your browser's status bar and see where it points to. Also, make sure you don't install any programs unless you know what they are and where they came from.

© *National Security Institute, Inc.*