SHIELD

Information Protection Newsletter

SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND

your energy partner®
OPPD
Omaha Public Power District

Protecting the keys to the kingdom

Passwords have rightly been called “the keys to the kingdom” by cyber security experts. Once hackers know your company login credentials, they can steal your personal information and also leverage your access rights to conduct more elaborate attacks by sending phishing email attacks to your contacts and use information found in your files to seriously harm OPPD.

The best thing you can do to protect your passwords is make them hard to guess and easy to remember. We recommend that you don’t use words found in dictionaries, even if they are foreign words. Lists created from dictionaries are standard parts of any password cracking software.

In previous issues of the ***SHIELD***, we’ve talked about creating passwords that are eight characters long and based on easy to remember phrases. Since these passwords are based on multiple words, hackers have an extremely difficult time guessing them.

The longer the phrase, the stronger the resulting password. Make sure you use at least a number, at least one upper case and at least one lower case letter, and at least a symbol in your passwords. For instance, you can use the phrase, “My pet alligator Elvis lives in an old bathtub,” to create the password “Mp@Elia0b” or the passphrase “My p3t @lligator Elvis lives an 0ld b@thtub.”

Don’t use a password for more than one site. For instance, if hackers guess that single password to crack your social media account, they will also use it against your online bank account and any e-commerce sites that might depend on the same credentials.

Do not under any circumstances share a password with others. Once you do that, the secret that protects your access to sensitive information is in someone else’s hands and whoever else they might decide to tell. If you suspect that someone else does know your password, change it immediately and inform the OPPD IT Service Desk.

Some sites now challenge you if you log in from an unexpected computer. For sites that use security questions to establish your identity, do not provide answers that can be found on your social media sites. Answers that might be discovered on social media sites include a pet’s names, the name of your best friend, and your mother’s maiden name.

Some sites now require two-factor authentication, where you enter a password and the site sends you a personal identification number via email or a SMS message. Other sites use artwork called captchas that may contain numbers or pictures. The best captchas so far depend on identifying or grouping pictures. For instance, you might be shown photos of food and asked which ones contain potatoes. Where possible, opt for a strong authentication method like the ones described above.

Do not write down your passwords and try to hide them somewhere on your desk. All the hiding places are well known and your passwords will be easily discovered.

Instead, use a password manager to store your passwords. Programs such as KeePass Password Safe keep lists of passwords encrypted and safe from prying eyes. Password managers are now available for a variety of operating systems. The only down side is you must remember the master password used to open the password manager.

Be wary of phishing attacks intended to steal your login credentials. Phishing attacks posing as Google Docs or Dropbox notifications are commonly used to get you to enter your email account and password supposedly in order to retrieve an unexpected but important document. This type of attack is quite common, odds are someone you know has encountered it.

You might get a phone call from someone claiming to belong to a technical support organization. This person will claim that your PC is causing problems on the internet and they need access to your PC in order to fix the problem. They will usually ask for you user ID and password in order to access your PC. After planting malicious software on your PC to harvest sensitive information they will use the credentials you game them to attack your online accounts.

Finally, if you encounter any of these attacks or find that your OPPD account is unexpectedly locked, contact the OPPD IT Service Desk immediately. Your reports are vital in keeping our sensitive information secure.

Use Email Safely

Email is the number one method cyber criminals use to attack their victims. Be suspicious of odd emails or emails that seem too good to be true.

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us at:

OPPD IT Service Desk

At home or at work

Protect your Internet Browsers

Hackers are targeting Internet browsers on desktops, laptops, smartphones, and tablet for all operating systems. Follow these security principles to keep your devices safe.

Ensure you are using the latest version of your Internet browser on all devices at home or at work. Internet browser developers are continually adding new features and security measures. In addition they are continually patching their work as hackers find new ways to exploit software weaknesses.

Where possible, avoid using plugins, also known as add-ons. While plugins help to add functionality to your Internet browser, they also add many new vulnerabilities that hackers routinely exploit. You will have to depend on the plugin maker to update them. If you must use a plugin, ensure that it can be updated automatically. Check the plugin web site regularly for security advisories and patching information.

Scan everything you download. Use your regularly updated anti-virus scanner to inspect every file or program your download before you open them.

Enable all browser security features for your Internet browser and search engines. It's a good idea to periodically check your Internet browser's security features. For instance, in Internet Explorer, ensure that Smartscreen Filter feature is turned on. For Google Search, in the Search Settings options, ensure that SafeSearch is turned on and locked. If you have doubts about a site, you can use the Google SafeBrowsing URL. For instance if you want to check out Google.com, enter the URL http://www.google.com/safebrowsing/diagnostic?site=google.com to return a report about the web domain. Just change the "site=" portion of the URL to check out a new do-

Browsing

Always ensure the browser you are using is the latest version, your plugins are up-to-date and scan any files you download with anti-virus.

your energy partner
OPPD
Omaha Public Power District

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us at:

OPPD IT Service Desk

North American Electric Reliability Corporation (NERC)

(Quarterly Update)

CIP-004 -3 R1- Security Awareness

Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

Direct communications (e.g., emails, memos, computer based training, etc.);

Indirect communications (e.g., posters, intranet, brochures, etc.)

Management support and reinforcement (e.g., presentations, meetings, etc.).

The responsibility of cyber security falls upon each and every individual within an organization. Today's hackers often target system deficiencies and software exploits, but the most effective method to interject viruses and gain access to protected information is perform by targeting personnel though email or social media. Hackers will often target personnel through "phishing" attacks and gain access after the user has opened the infected attachment or accesses a malicious website. OPPD has continued to defend against these highly crafted planned attacks by implementing a very robust cyber security awareness program. Annual training within interactive scenarios, consistent cyber security related articles posted on OPPD News, cyber security related posters and OPPD's SHIELD newsletter are a few of the methods used to strengthen OPPD's stance on protecting the organizations cyber assets.

For more information on OPPD's cyber security awareness program please visit the OPPD Cyber Security Awareness site.

If you have any questions or require any additional information regarding OPPD's Cyber Security Awareness Program please contact K.C. Carnes, Supervisor Cyber Security and Information Protection. For questions regarding OPPD's NERC CIP Program please contact Michael Nickels – OPPD Reliability Compliance Specialist.